Utilizzare le procedure ottimali per Secure Web Appliance

Sommario

Introduzione

In questo documento vengono descritte le best practice per configurare Cisco Secure Web Appliance (SWA).

Premesse

Questa guida è stata concepita come riferimento per la configurazione delle procedure ottimali e affronta molti aspetti di un'installazione SWA, tra cui l'ambiente di rete supportato, la configurazione delle policy, il monitoraggio e la risoluzione dei problemi. Anche se le best practice qui documentate sono importanti per la

comprensione di tutti gli amministratori, gli architetti e gli operatori, esse sono solo linee guida e devono essere trattate come tali. Ogni rete presenta esigenze e problematiche specifiche.

Come dispositivo di sicurezza, l'SWA interagisce con la rete in diversi modi unici. È sia un'origine che una destinazione del traffico web; agisce allo stesso tempo come un server web e un client web. Utilizza come minimo tecniche di spoofing degli indirizzi IP sul lato server e man-in-the-middle per ispezionare le transazioni HTTPS. Può inoltre eseguire lo spoofing degli indirizzi IP dei client, che aggiunge un altro livello di complessità all'installazione e impone requisiti aggiuntivi sulla configurazione di rete di supporto. Questa guida affronta i problemi più comuni relativi alla configurazione del dispositivo di rete correlato.

La configurazione della policy SWA ha implicazioni non solo sull'efficacia e l'applicazione della sicurezza, ma anche sulle prestazioni dell'accessorio. In questa guida viene illustrato l'impatto della complessità di una configurazione sulle risorse di sistema. Definisce la complessità in questo contesto e descrive come ridurla al minimo nella progettazione delle policy. Viene inoltre prestata attenzione alle caratteristiche specifiche e alla relativa configurazione per aumentare la sicurezza, la scalabilità e l'efficacia.

Nella sezione Monitoraggio e avvisi di questo documento vengono illustrati i metodi più efficaci per monitorare l'accessorio e viene descritto anche il monitoraggio delle prestazioni e della disponibilità, nonché l'utilizzo delle risorse di sistema. Fornisce inoltre informazioni utili per la risoluzione dei problemi di base.

Ambiente di rete

ICMP

Path MTU Discovery, come definito nella RFC 1191, determina le dimensioni massime di un pacchetto lungo percorsi arbitrari. Nel caso dell'IPv4, un dispositivo può determinare l'MTU (Maximum Transmission Unit) di un pacchetto lungo un percorso impostando il bit "non frammentare" (DF, Don't Fragment) nell'intestazione IP del pacchetto. Se in corrispondenza di un collegamento lungo il percorso un dispositivo non è in grado di inoltrare il pacchetto senza frammentarlo, all'origine viene inviato un messaggio **ICMP (Internet Control Message Protocol) necessario per** la **frammentazione (tipo 3, codice 4)**. Il client invia quindi un pacchetto più piccolo. Questa operazione continua finché non viene individuata l'MTU del percorso completo. IPv6 non supporta la frammentazione e utilizza un messaggio ICMPv6 Packet Too Big (Type 2) per indicare l'impossibilità di inserire un pacchetto in un determinato collegamento.

Poiché il processo di frammentazione dei pacchetti può avere un impatto notevole sulle prestazioni di un flusso TCP, l'SWA utilizza il rilevamento della MTU del percorso. I messaggi ICMP menzionati devono essere abilitati nei dispositivi di rete interessati per consentire all'SWA di determinare l'MTU del proprio percorso sulla rete. Questo comportamento può essere disattivato nell'SWA che utilizza il comando **CLI (Command-Line Interface)**. In questo modo, l'MTU predefinita scende a 576 byte (per RFC 879), compromettendo gravemente le prestazioni. L'amministratore deve fare l'ulteriore passo per configurare manualmente l'MTU nell'SWA da `etherconfig` CLI.

Nel caso del **protocollo WCCP (Web Cache Communication Protocol)**, il traffico Web viene reindirizzato all'SWA da un altro dispositivo di rete lungo il percorso client verso Internet. In questo caso, gli altri protocolli, ad esempio ICMP, non vengono reindirizzati all'SWA. È possibile che il dispositivo SWA attivi un messaggio ICMP Fragmentation Needed (Frammentazione richiesta ICMP) da un router della rete, ma il messaggio non verrà recapitato al dispositivo SWA. Se la rete supporta questa funzionalità, il rilevamento dell'MTU del percorso deve essere disabilitato. Come accennato, con questa configurazione,

l'ulteriore passaggio per impostare manualmente l'MTU sull'SWA da `etherconfig` Il comando CLI è obbligatorio.

Firewall

In una configurazione predefinita, l'SWA non effettua lo spoofing dell'indirizzo IP del client quando inoltra una connessione. Ciò significa che tutto il traffico Web in uscita proviene dall'indirizzo IP SWA. È necessario verificare che i dispositivi **Network Address Translation (NAT)** dispongano di un pool sufficiente di indirizzi e porte esterni per supportare questa condizione. A tal fine è opportuno dedicare un indirizzo specifico.

Alcuni firewall utilizzano protezioni **DoS (Denial-of-Service)** o altre funzionalità di sicurezza che vengono attivate quando un numero elevato di connessioni simultanee viene originato da un singolo indirizzo IP del client. Quando lo spoofing IP del client non è abilitato, l'indirizzo IP SWA deve essere escluso da queste protezioni.

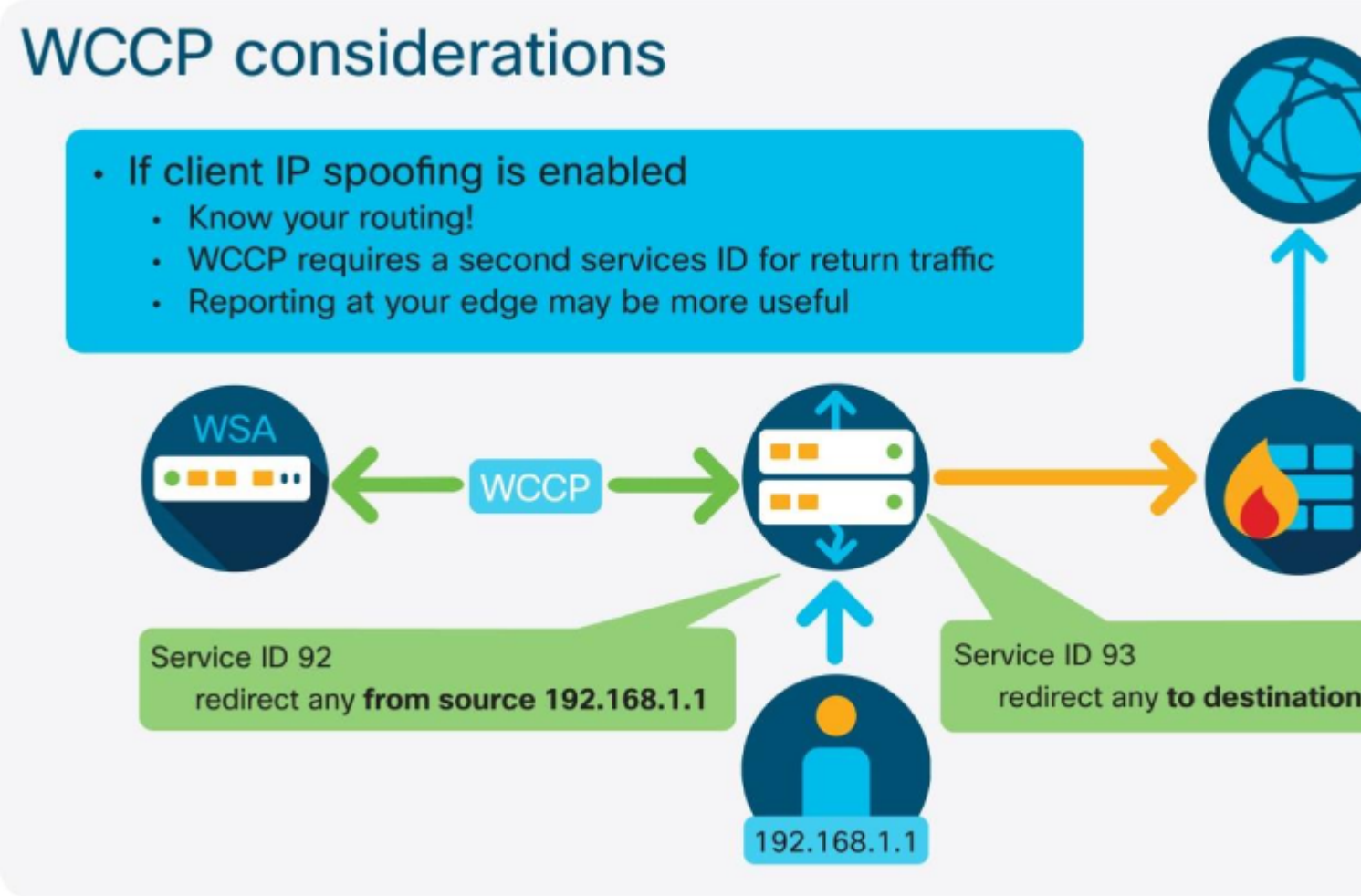
Inoltro percorso inverso unicast

Il SWA falsifica l'indirizzo IP del server quando comunica con un client e può essere configurato per falsificare l'indirizzo IP del client quando comunica con un server upstream. Sugli switch è possibile abilitare protezioni quali **Unicast Reverse Path Forwarding (uRPF)** per assicurare che un pacchetto in arrivo corrisponda alla porta in entrata prevista. Queste protezioni controllano l'interfaccia di origine di un pacchetto rispetto alla tabella di routing per verificare che sia arrivato sulla porta prevista. Se del caso, la SWA deve essere esentata da tali protezioni.

Spoofing IP con WCCP

Quando la funzione di spoofing IP è attivata nell'interfaccia SWA, le richieste in uscita lasciano all'accessorio l'indirizzo di origine della richiesta client originale. Ciò richiede una configurazione aggiuntiva dell'infrastruttura di rete correlata per garantire che i pacchetti restituiti vengano instradati all'interfaccia SWA in uscita, anziché al client da cui proviene la richiesta.

Quando si implementa WCCP su un dispositivo di rete (router, switch o firewall), viene definito un ID servizio che corrisponde al traffico in base a un **Access Control List (ACL)**. L'ID servizio viene quindi applicato a un'interfaccia e utilizzato per associare il traffico al reindirizzamento. Se lo spoofing IP è abilitato, è necessario creare un secondo ID servizio per garantire che anche il traffico di ritorno venga reindirizzato all'SWA.



Configurazione rete SWA

Interfacce

L'SWA ha cinque interfacce di rete utilizzabili: M1, P1, P2, T1 e T2. Ognuno di questi deve essere sfruttato per il proprio scopo specifico, quando possibile. L'utilizzo di ciascuna porta è utile per le proprie ragioni. L'interfaccia M1 deve essere connessa a una rete di gestione dedicata e deve essere abilitato il split-routing per limitare l'esposizione dei servizi amministrativi. P1 può essere limitato al traffico di richieste del client, mentre P2 non può accettare richieste proxy esplicite. Ciò riduce la quantità di traffico su ciascuna interfaccia e consente una migliore segmentazione nella progettazione della rete.

Le porte T1 e T2 sono disponibili per la funzionalità **Layer 4 Traffic Monitor (L4TM)**. Questa funzionalità esegue il monitoraggio di una porta di livello 2 con mirroring e aggiunge la possibilità di bloccare il traffico in base a un elenco bloccato di indirizzi IP e nomi di dominio dannosi noti. A tale scopo, controlla gli indirizzi IP di origine e di destinazione del traffico e invia un pacchetto di reimpostazione TCP o un messaggio Port Unreachable se l'elenco degli indirizzi bloccati corrisponde. Questa funzione può bloccare il traffico inviato con qualsiasi protocollo.

Anche se la funzione L4TM non è attivata, è possibile migliorare il bypass trasparente quando le porte T1 e T2 sono collegate a una porta con mirroring. Nel caso della WCCP, il dispositivo SWA conosce solo l'indirizzo IP di origine e di destinazione di un pacchetto in arrivo e deve decidere se inoltrarlo o ignorarlo in base a tali informazioni. La SWA risolve tutte le voci nell'elenco delle impostazioni di bypass ogni 30 minuti, indipendentemente dal **TTL (Time to Live)** del record. Tuttavia, se la funzione L4TM è attivata,

l'SWA può utilizzare le query DNS snooped per aggiornare questi record con maggiore frequenza. Ciò riduce il rischio di un falso negativo in uno scenario in cui il client ha risolto un indirizzo diverso da quello dell'SWA.

Routing della rete di gestione

Se la rete di gestione dedicata non dispone di accesso a Internet, è possibile configurare ogni servizio per l'utilizzo della tabella di routing dei dati. Questo può essere personalizzato per adattarsi alla topologia di rete, ma in generale si consiglia di utilizzare la rete di gestione per tutti i servizi di sistema e la rete di dati per il traffico dei client. A partire dalla versione AsyncOS 11.0, i servizi per i quali è possibile impostare il routing sono:

- Feed URL esterni
- Reputazione e analisi dei file di **Advanced Malware Protection (AMP)**
- Aggiornamenti
- DNS
- Active Directory

Per ulteriori operazioni di filtro in uscita del traffico di gestione, è possibile configurare gli indirizzi statici da utilizzare nei seguenti servizi:

- Feed URL esterni:
  1. I servizi personalizzati dipendono dalla posizione in cui si trovano
  2. Reputazione e analisi dei file AMP
  3. cloud-sa.amp.cisco.com (Nord America)
  4. cloud-sa.eu.amp.cisco.com (Europa)
  5. cloud-sa.apjc.amp.cisco.com (Asia-Pacifico)

- Aggiornamenti:
  1. downloads-static.ironport.com
  2. updates-static.ironport.com

Telemetria TALOS

Il Cisco Talos Group è ben noto per aver identificato minacce nuove ed emergenti. Tutti i dati inviati a Talos sono anonimizzati e memorizzati nei centri dati statunitensi. La partecipazione a SensorBase migliora la classificazione e l'identificazione delle minacce Web e migliora la protezione da SWA e da altre soluzioni di sicurezza Cisco.

DNS

In base alle procedure consigliate per la sicurezza DNS (Domain Name Server), ogni rete deve ospitare due resolver DNS, uno per i record autorevoli di un dominio locale e uno per la risoluzione ricorsiva dei domini Internet. Per risolvere questo problema, l'SWA consente di configurare i server DNS per domini specifici. Se per le query locali e ricorsive è disponibile un solo server DNS, considerare il carico aggiuntivo aggiunto quando viene utilizzato per tutte le query SWA. L'opzione migliore può essere quella di utilizzare il resolver interno per i domini locali e i resolver Internet radice per i domini esterni. Ciò dipende dal profilo di rischio e dalla tolleranza dell'amministratore.

Per impostazione predefinita, l'SWA memorizza nella cache un record DNS per un minimo di 30 minuti, indipendentemente dal valore TTL del record. I siti Web moderni che fanno un uso intensivo delle **reti CDN (Content Delivery Network)** hanno bassi record TTL in quanto i loro indirizzi IP cambiano frequentemente. Ciò può comportare che un client memorizzi nella cache un indirizzo IP per un determinato server e che il provider di servizi condivisi memorizzi nella cache un indirizzo diverso per lo stesso server.

Per risolvere questo problema, il valore TTL predefinito SWA può essere ridotto a cinque minuti dai seguenti comandi CLI:

```
SWA_CLI> dnsconfig
...
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.
[]> SETUP
...
Enter the minimum TTL in seconds for DNS cache.
...
```

Se il server primario non è disponibile, è necessario configurare i server DNS secondari. Se tutti i server sono configurati con la stessa priorità, l'indirizzo IP del server viene scelto in modo casuale. A seconda del numero di server configurati, il timeout per un determinato server varia. La tabella indica il timeout per una query relativa a un massimo di sei server DNS:

Numero di server DNS	**Timeout query (in sequenza)**
1	60
2	5, 45
3	5, 10, 45
4	1, 3, 11, 45
5	1, 3, 11, 45, 1
6	1, 3, 11, 45, 1, 1

Sono inoltre disponibili opzioni DNS avanzate solo tramite la CLI. Queste opzioni sono disponibili nella CLI:

advancedproxyconfig > DNS Selezionare una delle opzioni seguenti:

- 0: utilizza sempre le risposte DNS in ordine
- 1: utilizzare l'indirizzo fornito dal client e quindi il DNS
- 2 - Utilizzo limitato di DNS
- 3 - Utilizzo DNS molto limitato

Per le opzioni 1 e 2, se è abilitata la reputazione Web viene utilizzato il DNS.

Per le opzioni 2 e 3, il DNS viene utilizzato per le richieste esplicite del proxy, se non è presente alcun proxy upstream o nel caso in cui il proxy upstream configurato abbia esito negativo.

Per tutte le opzioni, il DNS viene utilizzato quando gli indirizzi IP di destinazione vengono utilizzati nell'appartenenza ai criteri.

Queste opzioni controllano il modo in cui l'SWA decide l'indirizzo IP a cui connettersi durante la valutazione di una richiesta client. Quando riceve una richiesta, il SWA visualizza un indirizzo IP di destinazione e un nome host. L'SWA deve decidere se considerare attendibile l'indirizzo IP di destinazione originale per la connessione TCP o se eseguire la propria risoluzione DNS e utilizzare l'indirizzo risolto. L'impostazione predefinita è "0 = Utilizza sempre le risposte DNS in ordine", ovvero l'SWA non considera attendibile il client per fornire l'indirizzo IP.

- Opzione 1 - L'SWA tenta di utilizzare l'indirizzo IP fornito dal client per la connessione, ma se l'operazione non riesce, torna all'indirizzo risolto. L'indirizzo risolto viene utilizzato per la valutazione dei criteri (categoria Web, reputazione Web e così via).
- Opzione 2 - L'SWA utilizza solo l'indirizzo fornito dal client per la connessione e non esegue il fallback. L'indirizzo risolto viene utilizzato per la valutazione dei criteri (categoria Web, reputazione Web e così via).
- Opzione 3 - L'SWA utilizza solo l'indirizzo fornito dal client per la connessione e non esegue il fallback. L'indirizzo IP fornito dal client viene utilizzato per la valutazione dei criteri (categoria Web, reputazione Web e così via).

L'opzione scelta dipende dal livello di attendibilità che l'amministratore deve porre nel client quando determina l'indirizzo risolto per un determinato nome host. Se il client è un proxy downstream, scegliere l'opzione 3 per evitare l'aggiunta della latenza di ricerche DNS non necessarie.

Bilanciamento del carico

WCCP consente il bilanciamento trasparente del carico del traffico quando vengono utilizzati fino a otto appliance. Consente di bilanciare i flussi di traffico in base all'hash o alla maschera, può essere ponderato in caso di combinazione di modelli di appliance nella rete e i dispositivi possono essere aggiunti e rimossi dal pool di servizi senza tempi di inattività. Quando la necessità supera quanto è possibile gestire con otto SWA, si consiglia di utilizzare un load balancer dedicato.

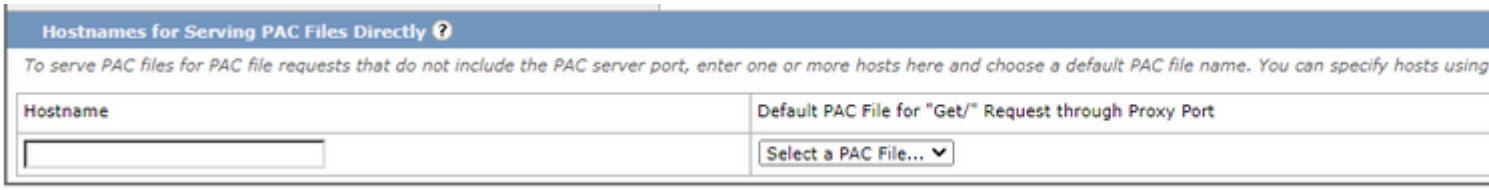
Le best practice specifiche per la configurazione di WCCP variano in base alla piattaforma utilizzata. Per gli switch Cisco Catalyst®, le best practice sono documentate nel white paper sulla soluzione Cisco Catalyst Instant Access.

L'uso di WCCP con Cisco Adaptive Security Appliance (ASA) è limitato. In altre parole, lo spoofing IP dei client non è supportato e i client e l'interfaccia SWA devono trovarsi dietro la stessa interfaccia. Per questo motivo, è più flessibile utilizzare uno switch o un router di layer 4 per reindirizzare il traffico. La configurazione WCCP sulla piattaforma ASA è descritta in WCCP sull'appliance ASA: concetti, limitazioni e configurazione.

Per le distribuzioni esplicite, un file di configurazione automatica dei proxy (PAC) è il metodo più diffuso, ma presenta molti inconvenienti e implicazioni per la sicurezza che esulano dall'ambito di questo documento. Se viene distribuito un file PAC, è consigliabile utilizzare gli oggetti Criteri di gruppo per configurare il percorso anziché utilizzare il protocollo WPAD (Web Proxy Autodiscover Protocol), che è una destinazione comune per gli utenti malintenzionati e può essere facilmente sfruttato in caso di configurazione errata. L'SWA può ospitare più file PAC e controllarne la scadenza nella cache del browser.

Un file PAC può essere richiesto direttamente dall'SWA da un numero di porta TCP configurabile (9001 per impostazione predefinita). Se non si specifica una porta, la richiesta può essere inviata al processo proxy

stesso come se fosse una richiesta Web in uscita. In questo caso, è possibile utilizzare un file PAC specifico basato sull'intestazione host HTTP presente nella richiesta.



Kerberos deve essere configurato in modo diverso quando viene utilizzato in un ambiente ad alta disponibilità. L'SWA fornisce il supporto per i file keytab, che consente l'associazione di più nomi host a un **SPN (Service Principle Name)**. Per ulteriori informazioni, vedere Creazione di un account di servizio in Windows Active Directory per l'autenticazione Kerberos nelle distribuzioni ad alta disponibilità.

Autenticazione attiva

Kerberos è un protocollo di autenticazione più sicuro e ampiamente supportato rispetto a **NTLMSSP (NT LAN Manager Security Support Provider)**. Il sistema operativo Apple OS X non supporta NTLMSSP, ma può utilizzare Kerberos per eseguire l'autenticazione se il dominio viene aggiunto. L'autenticazione di base non deve essere utilizzata, in quanto invia credenziali non crittografate nell'intestazione HTTP e può essere facilmente rilevata da un utente non autorizzato sulla rete. Se è necessario utilizzare l'autenticazione di base, è necessario abilitare la crittografia delle credenziali per garantire l'invio delle credenziali in un tunnel crittografato.

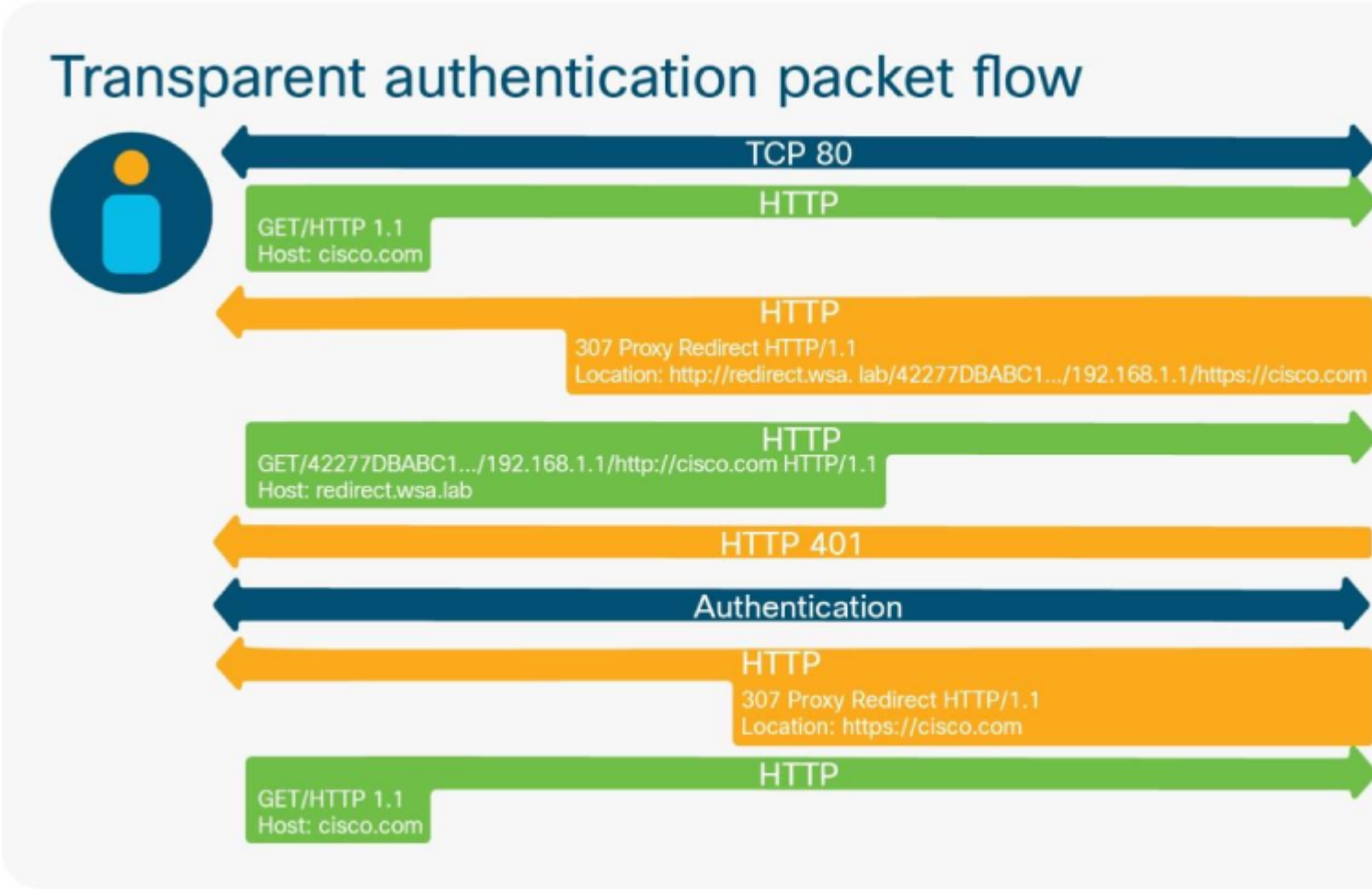
Per garantire la disponibilità, è necessario aggiungere alla configurazione più controller di dominio, ma non è presente alcun bilanciamento del carico intrinseco del traffico. L'SWA invia un pacchetto TCP SYN a tutti i controller di dominio configurati e il primo a rispondere viene utilizzato per l'autenticazione.

Il "reindirizzamento del nome host" configurato nella pagina delle impostazioni di autenticazione determina la posizione in cui viene inviato un client trasparente per completare l'autenticazione. Affinché un client Windows possa completare l'autenticazione integrata e ottenere l'**SSO (Single Sign-On)**, il nome host di reindirizzamento deve trovarsi nell'area "Siti attendibili" del Pannello di controllo "Opzioni Internet". Il protocollo Kerberos richiede l'utilizzo del **nome di dominio completo (FQDN)** per specificare una risorsa. Questo significa che il nome "shortname" (o "NETBIOS") non può essere utilizzato se Kerberos è il meccanismo di autenticazione previsto. L'FQDN deve essere aggiunto manualmente ai "Siti attendibili" (ad esempio tramite Criteri di gruppo). Inoltre, l'accesso automatico con nome utente e password deve essere impostato in "Opzioni Internet" nel Pannello di controllo.

In Firefox sono inoltre necessarie impostazioni aggiuntive per consentire al browser di completare l'autenticazione con i proxy di rete. Queste impostazioni possono essere configurate nella pagina **about:config**. Per completare correttamente Kerberos, è necessario aggiungere il nome host di reindirizzamento all'opzione **network.negotiation-auth.trusted-uris**. Per NTLMSSP, è necessario aggiungerlo all'opzione **network.automatic-ntlm-auth.trusted-uris**.

I surrogati di autenticazione vengono utilizzati per ricordare un utente autenticato per una determinata durata al termine dell'autenticazione. Ove possibile, è necessario utilizzare i surrogati IP per limitare il numero di eventi di autenticazione attivi che si verificano. L'autenticazione attiva di un client è un'attività che richiede molte risorse, in particolare quando si utilizza Kerberos. Per impostazione predefinita, il timeout del surrogato è di 3600 secondi (un'ora) e può essere ridotto, ma il valore più basso consigliato è 900 secondi (15 minuti).

Nell'immagine viene mostrato come usare "redirect.WSA.lab" come nome host di reindirizzamento.



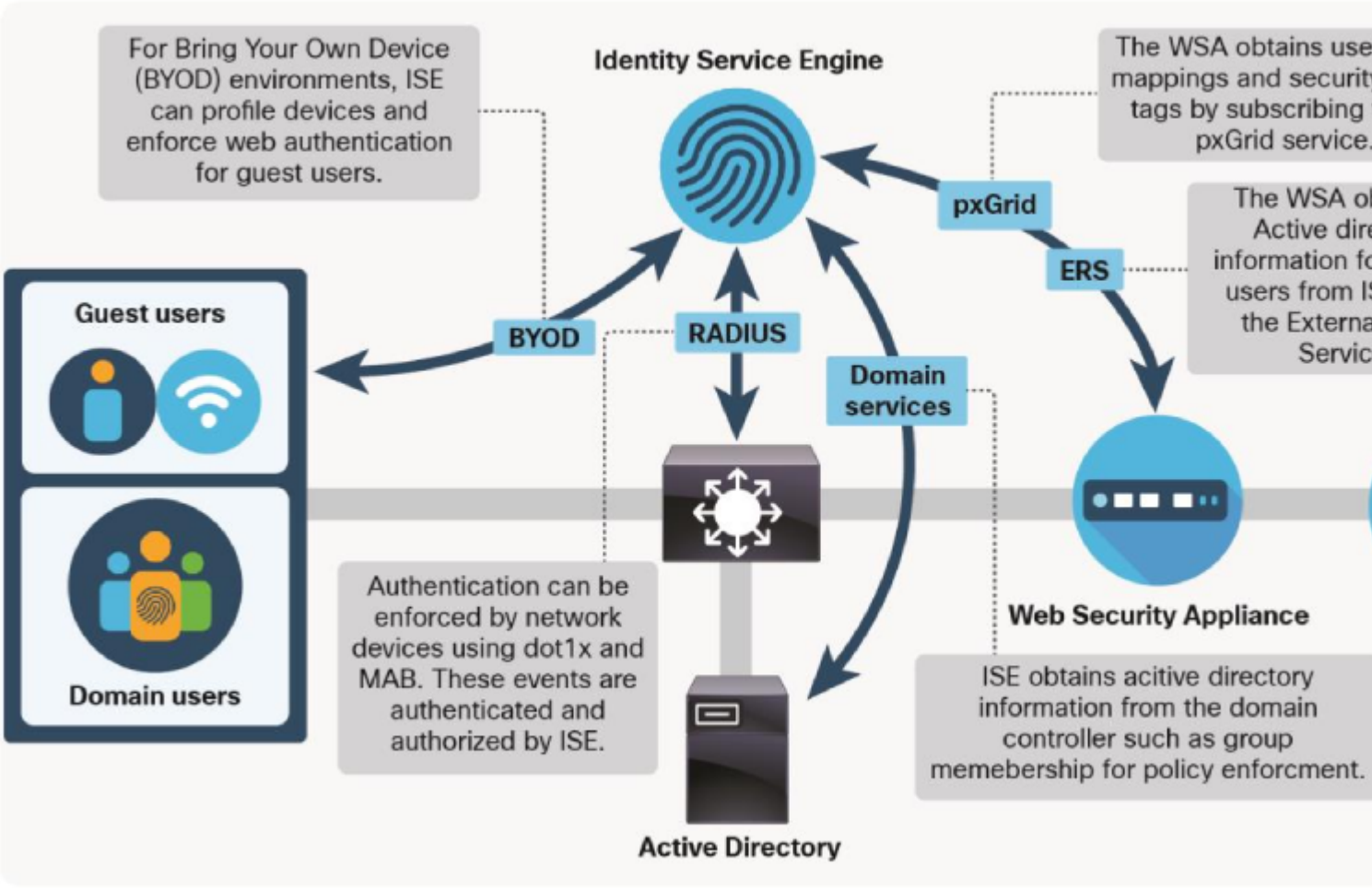
Autenticazione passiva

Il dispositivo SWA può utilizzare altre piattaforme di sicurezza Cisco per identificare in modo passivo gli utenti proxy. L'identificazione passiva degli utenti elimina la necessità di una richiesta di autenticazione diretta e di qualsiasi comunicazione di Active Directory da parte dell'SWA, riducendo così la latenza e l'utilizzo delle risorse sull'accessorio. I meccanismi attualmente disponibili per l'autenticazione passiva sono **CDA (Context Directory Agent)**, **Identity Services Engine (ISE)** e **ISE-PIC (Identity Services Connector Passive Identity Connector)**.

ISE è un prodotto ricco di funzionalità che aiuta gli amministratori a centralizzare i servizi di autenticazione e a sfruttare un'ampia gamma di controlli dell'accesso alla rete. Quando ISE viene a conoscenza di un evento di autenticazione dell'utente (tramite l'autenticazione Dot1x o il reindirizzamento dell'autenticazione Web), popola un database di sessione contenente informazioni sull'utente e sul dispositivo coinvolti nell'autenticazione. L'SWA si connette ad ISE sulla **Platform Exchange Grid (pxGrid)** e ottiene il nome utente, l'indirizzo IP e il codice di matricola (SGT) associati a una connessione proxy. A partire dalla versione AsyncOS 11.7, il SWA può anche richiedere informazioni sul gruppo al **External Restful Service (ERS)** su ISE.

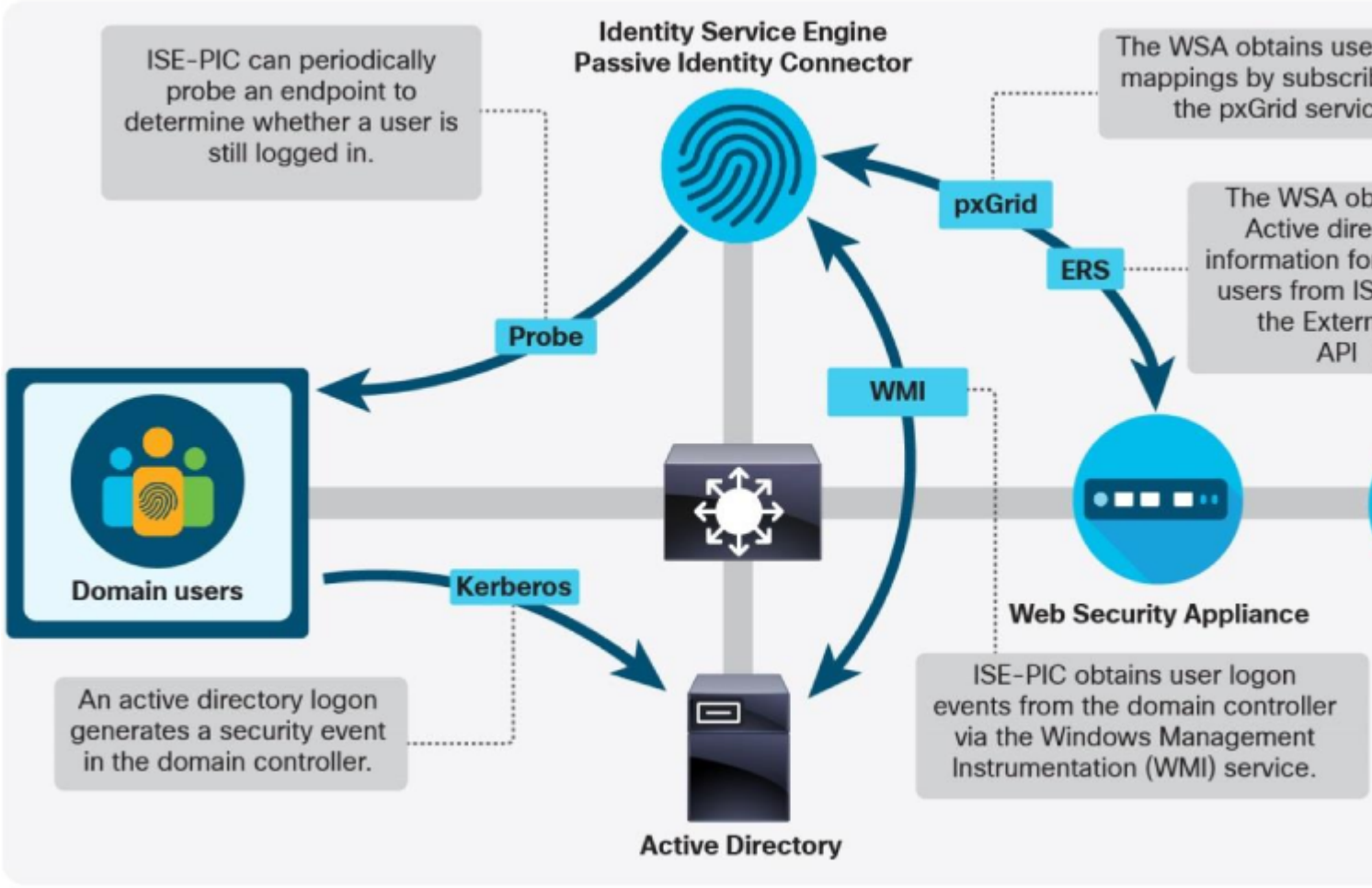
Le versioni suggerite sono ISE 3.1 e SWA 14.0.2-X e successive. Per ulteriori informazioni sulla matrice di compatibilità ISE per SWA, vedere ISE Compatibility Matrix per Secure Web Appliance.

Per ulteriori informazioni sulla procedura di integrazione completa, vedere la Guida dell'utente finale di Web Security Appliance.



Cisco annuncia la fine del ciclo di vita del software Cisco Context Directory Agent (CDA), vedere Cisco Context Directory Agent (CDA).

A partire dalla patch 6 CDA, è compatibile con Microsoft Server 2016. Tuttavia, gli amministratori sono attivamente incoraggiati a migrare le loro implementazioni CDA ad ISE-PIC. Entrambe le soluzioni utilizzano WMI per sottoscrivere il registro eventi di protezione di Windows per generare mapping utente-IP (noti come "sessioni"). Nel caso di CDA, l'SWA interroga queste mappature con RADIUS. Nel caso di ISE-PIC, vengono utilizzate le stesse connessioni pxGrid e ERS utilizzate nell'implementazione completa di ISE. La funzionalità ISE-PIC è disponibile in un'installazione completa ISE e in un dispositivo virtuale indipendente.

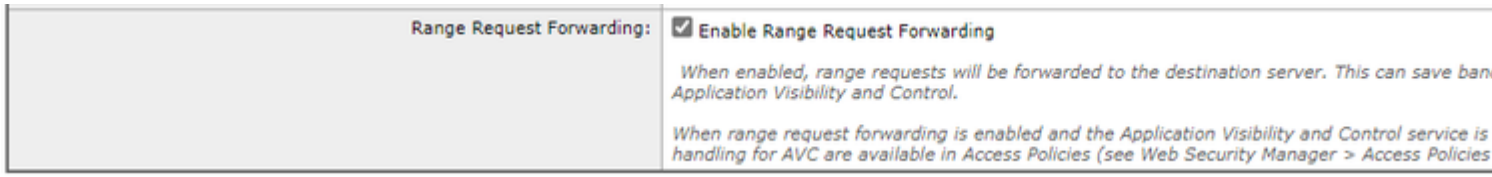


Configurazione servizi

Proxy Web

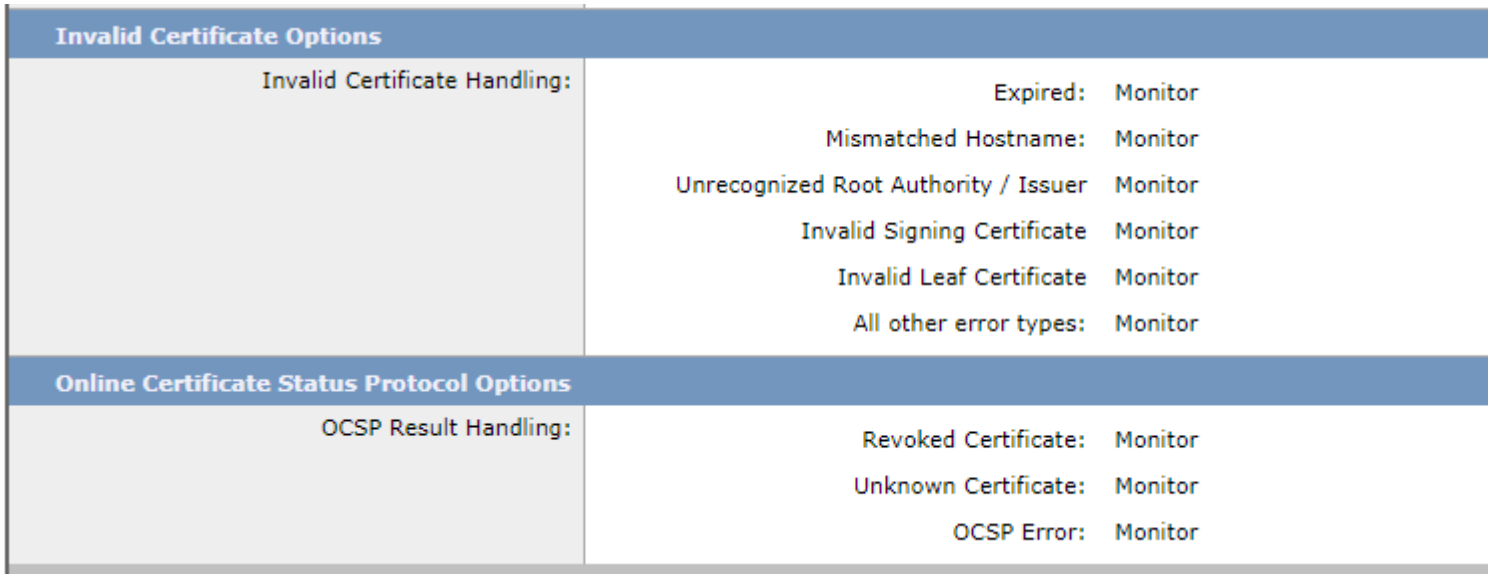
La memorizzazione nella cache deve essere abilitata nella configurazione del proxy Web per risparmiare larghezza di banda e migliorare le prestazioni. Questa operazione sta diventando meno importante con l'aumento della percentuale di traffico HTTPS perché l'SWA non memorizza nella cache le transazioni HTTPS per impostazione predefinita. Se il proxy viene distribuito per servire solo i client espliciti, è necessario specificare la modalità di inoltro per rifiutare qualsiasi traffico non destinato in modo specifico al servizio proxy. In questo modo, la superficie di attacco dell'accessorio viene ridotta e viene applicato un buon principio di sicurezza: spegnerlo se non è necessario.

Le intestazioni di richiesta Range vengono utilizzate nelle richieste HTTP per specificare l'intervallo di byte di un file da scaricare. Viene comunemente utilizzato dai daemon di aggiornamento del sistema operativo e delle applicazioni per trasferire piccole porzioni di un file alla volta. Per impostazione predefinita, il SWA rimuove queste intestazioni in modo da ottenere l'intero file per la scansione antivirus (AV), la reputazione e l'analisi dei file e **l'AVC (Application Visibility Control)**. L'abilitazione dell'inoltro delle intestazioni delle richieste di intervallo a livello globale nelle impostazioni proxy consente agli amministratori di creare criteri di accesso individuali per l'inoltro o l'eliminazione di tali intestazioni. Per ulteriori informazioni su questa configurazione, vedere la sezione **Criteri di accesso**.



Proxy HTTPS

In base alle best practice sulla sicurezza, le chiavi private devono essere generate sull'accessorio in cui vengono utilizzate e non devono mai essere trasferite altrove. La procedura guidata del proxy HTTPS consente di creare la coppia di chiavi e il certificato utilizzati per la decrittografia delle connessioni **TLS (Transport Layer Security)**. La **richiesta di firma del certificato (CSR)** può quindi essere scaricata e firmata da un'**autorità di certificazione (CA)** interna. In un ambiente **Active Directory (AD)** questo è il metodo migliore, in quanto una CA integrata in Active Directory viene considerata automaticamente attendibile da tutti i membri del dominio e non richiede passaggi aggiuntivi per distribuire il certificato. Una funzione di sicurezza del proxy HTTPS consiste nel convalidare i certificati del server. In base alle procedure consigliate, per i certificati non validi è necessario eliminare la connessione. L'attivazione di Decrypt for EUN consente all'SWA di presentare una pagina che spiega il motivo del blocco. Se questa opzione non è attivata, tutti i siti HTTPS bloccati genereranno un errore del browser. Ciò ha portato a un aumento dei biglietti per l'help desk e alla supposizione da parte dell'utente che qualcosa si è rotto, piuttosto che alla consapevolezza che la SWA ha bloccato la connessione. Tutte le opzioni del certificato non valide devono essere impostate almeno su Decrittografa. Se queste opzioni vengono lasciate come Monitor, non sarà possibile registrare messaggi di errore utili nel caso in cui problemi relativi ai certificati impediscano il caricamento di un sito.



Analogamente, è necessario lasciare attivati i controlli **OCSP (Online Certificate Services Protocol)** e non utilizzare Monitor per alcuna opzione. I certificati revocati devono essere eliminati e tutti gli altri devono essere almeno impostati su Decrittografa per consentire la registrazione dei messaggi di errore rilevanti. **La ricerca di informazioni sull'autorità (AIA, Authority Information Access Chasing)** è uno strumento tramite il quale un client può ottenere il firmatario del certificato e un URL dal quale è possibile recuperare ulteriori certificati. Ad esempio, se una catena di certificati ricevuta da un server è incompleta (manca un certificato intermedio o radice), l'SWA può controllare il campo AIA e utilizzarlo per recuperare i certificati mancanti e verificarne l'autenticità. Questa impostazione è disponibile solo nella CLI da questi comandi:

```
SWA_CLI> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
```

```
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
- CONTENT-ENCODING - Block content-encoding types
- SCANNERS - Scanner related parameters
[]> HTTPS
...
Do you want to enable automatic discovery and download of missing Intermediate Certificates?
[Y]>
...
```

> **Nota**: questa impostazione è abilitata per impostazione predefinita e non deve essere disabilitata, in quanto molti server moderni si basano su questo meccanismo per fornire una catena di attendibilità completa ai client.

L4TM (Layer 4 Traffic Monitor)

L4TM è un modo molto efficace per estendere la portata dell'SWA in modo da includere il traffico dannoso che non attraversa il proxy, compreso il traffico su tutte le porte TCP e UDP. Le porte T1 e T2 sono destinate a essere collegate a un collegamento di rete o a una sessione di monitoraggio dello switch, che consente a SWA di monitorare passivamente tutto il traffico proveniente dai client. Se viene rilevato traffico destinato a un indirizzo IP dannoso, il servizio SWA può terminare le sessioni TCP inviando un RST durante lo spoofing dell'indirizzo IP del server. Per il traffico UDP, può inviare un messaggio Port Unreachable (Porta non raggiungibile). Quando si configura la sessione di monitoraggio, è consigliabile escludere qualsiasi traffico destinato all'interfaccia di gestione dell'SWA per evitare che la funzione possa interferire con l'accesso al dispositivo.
Oltre a monitorare il traffico dannoso, L4TM interrompe anche le query DNS per aggiornare l'elenco delle impostazioni di bypass. Questo elenco viene utilizzato nelle distribuzioni WCCP per restituire alcune richieste al router WCCP per il routing diretto al server Web. I pacchetti che corrispondono all'elenco delle impostazioni di bypass non vengono elaborati dal proxy. L'elenco può contenere indirizzi IP o nomi di server. Il SWA risolve tutte le voci nell'elenco delle impostazioni di bypass ogni 30 minuti, indipendentemente dal valore TTL del record. Tuttavia, se la funzione L4TM è attivata, l'SWA può utilizzare le query DNS snooped per aggiornare questi record con maggiore frequenza. Ciò riduce il rischio di un falso negativo in uno scenario in cui il client ha risolto un indirizzo diverso da quello dell'SWA.

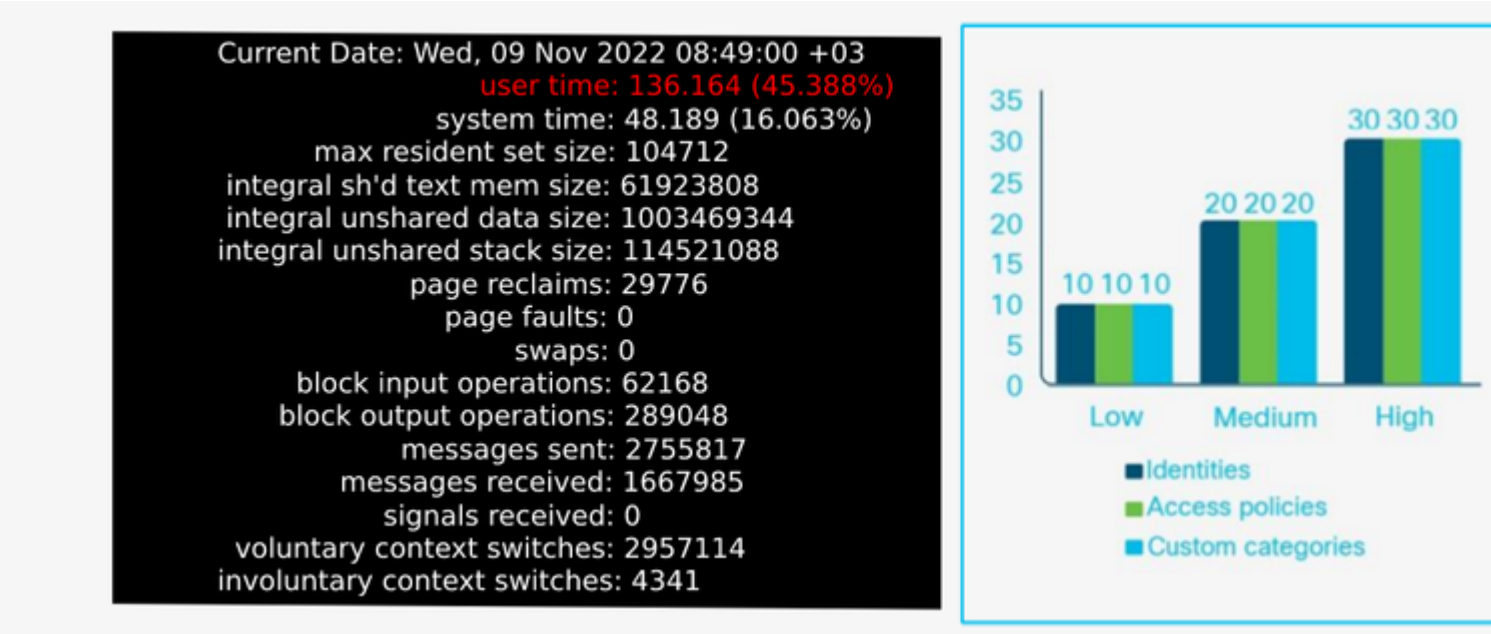
Configurazione criteri

La corretta configurazione delle policy è fondamentale per le prestazioni e la scalabilità del SWA. Ciò è vero non solo per l'efficacia delle politiche stesse nel proteggere i clienti e nel far rispettare i requisiti aziendali. Il modo in cui le policy vengono configurate ha un impatto diretto sull'utilizzo delle risorse e sullo stato e sulle prestazioni generali dell'SWA. Un insieme di regole troppo complesso o mal progettato può causare instabilità e rallentare i tempi di risposta dell'accessorio.

Complessità

Nella definizione delle politiche SWA vengono utilizzati vari elementi politici. Il file XML generato dalla configurazione viene utilizzato per creare diversi file di configurazione back-end e regole di accesso. Più la configurazione è complessa, maggiore è il tempo che il processo proxy impiega per valutare i vari set di regole per ogni transazione. Nel benchmarking e nel dimensionamento dell'SWA, viene creato un insieme di

elementi di base che rappresentano tre livelli di complessità della configurazione. Dieci profili di identità, criteri di decrittografia e criteri di accesso, insieme a dieci categorie personalizzate contenenti dieci voci regex, cinquanta indirizzi IP server e 420 nomi host server, è considerata una configurazione a bassa complessità. La moltiplicazione di ognuna di queste cifre per due e tre genera rispettivamente una configurazione di complessità media e una configurazione di complessità elevata.
Quando una configurazione diventa troppo complessa, i primi sintomi in genere includono una risposta lenta nell'interfaccia Web e nella CLI. Inizialmente non vi può essere un impatto significativo per gli utilizzatori. Tuttavia, più complessa è la configurazione, maggiore è il tempo che il processo proxy deve dedicare in modalità utente. Per questo motivo, controllare la percentuale di tempo trascorso in questa modalità può essere un modo utile per diagnosticare una configurazione eccessivamente complessa come causa di un SWA lento.
Il tempo CPU, in secondi, viene registrato nel registro track_stats ogni cinque minuti. Ciò significa che la percentuale di tempo utente può essere calcolata come (tempo utente + tempo di sistema)/300. Con il tempo utente che si avvicina a 270, il processo impiega troppi cicli della CPU in modalità utente, e questo accade quasi sempre perché la configurazione è troppo complessa per essere analizzata in modo efficiente.



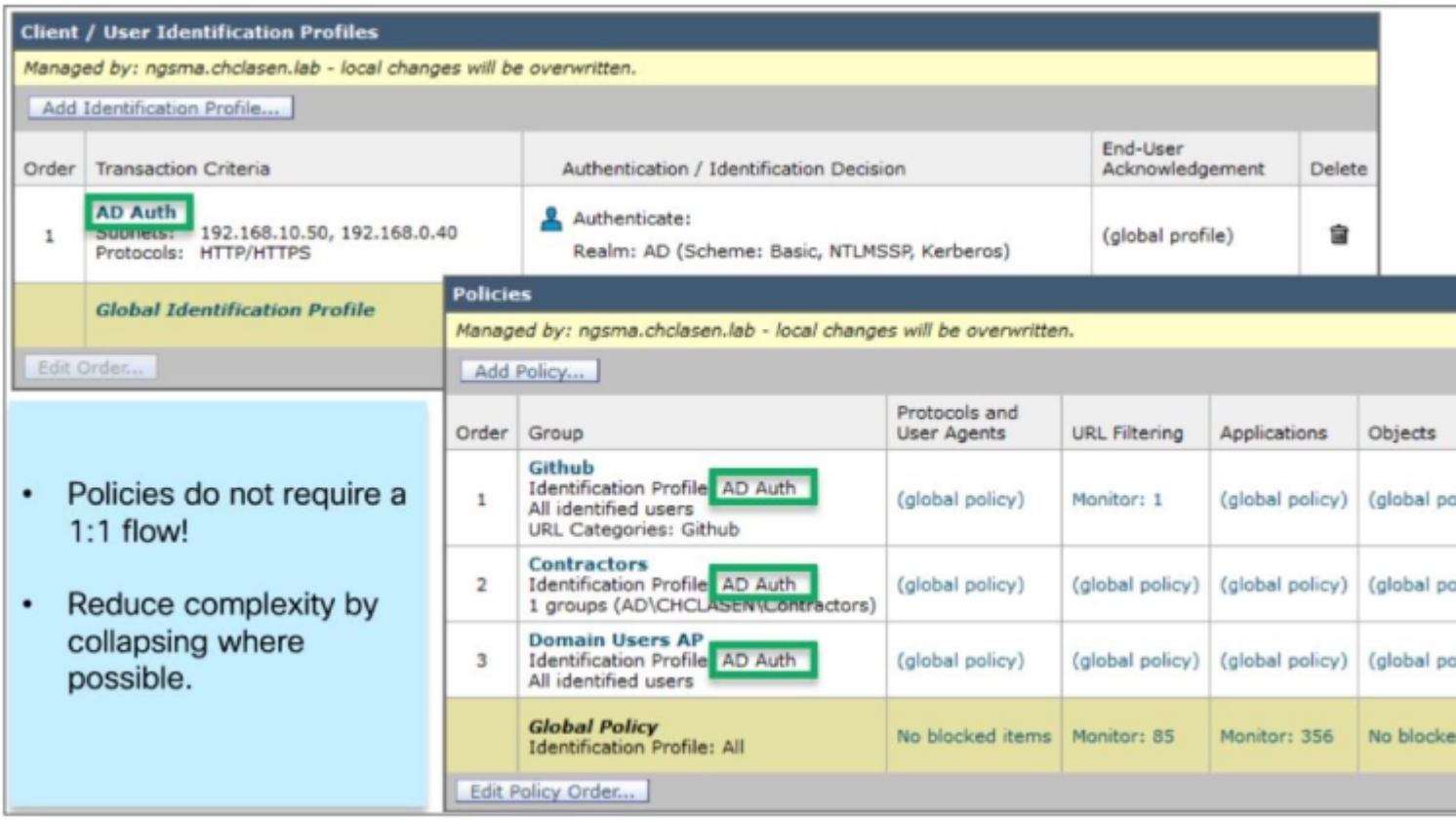
Profili di identificazione

I profili di identificazione (ID) sono i primi elementi dei criteri valutati quando viene ricevuta una nuova richiesta. Tutte le informazioni configurate nella prima sezione del profilo ID vengono valutate con un AND logico. Ciò significa che tutti i criteri devono corrispondere affinché la richiesta corrisponda al profilo. Quando si crea una politica, questa deve essere tanto specifica quanto assolutamente necessaria. I profili che includono singoli indirizzi host non sono quasi mai necessari e possono portare a configurazioni estese. L'utilizzo della stringa agente utente presente nelle intestazioni HTTP, nell'elenco di categorie personalizzate o nella subnet rappresenta in genere una strategia migliore per limitare l'ambito di un profilo.

In generale, i criteri che richiedono l'autenticazione vengono configurati nella parte inferiore e sopra di essi vengono aggiunte le eccezioni. Quando si ordinano i criteri che non richiedono l'autenticazione, i criteri più utilizzati devono essere i più vicini possibili all'inizio. Non fare affidamento sull'autenticazione non riuscita per limitare l'accesso. Se è noto che un client della rete non è in grado di eseguire l'autenticazione a un proxy, è necessario esentarlo dall'autenticazione e bloccarlo nei criteri di accesso. I client che non possono eseguire ripetute autenticazioni inviano richieste non autenticate al SWA, che utilizza risorse e può causare un utilizzo eccessivo della CPU e della memoria.

Un'errata concezione comune per gli amministratori è che devono esistere un profilo ID univoco e criteri di

decrittografia e di accesso corrispondenti. Si tratta di una strategia inefficiente per la configurazione delle policy. Quando possibile, i criteri devono essere "compressi" in modo che un singolo profilo ID possa essere associato a più criteri di accesso e decrittografia. Ciò è possibile perché tutti i criteri in un determinato criterio devono corrispondere affinché il traffico corrisponda al criterio. Essendo più generici nei criteri di autenticazione e più specifici nei criteri risultanti, è possibile ridurre il numero complessivo di criteri.



Criteri di decrittografia

Come per il profilo ID, anche i criteri impostati nei criteri di decrittografia vengono valutati come AND logico, con un'importante eccezione quando vengono utilizzate informazioni provenienti dall'ISE. Di seguito viene illustrato il funzionamento della corrispondenza dei criteri, a seconda degli elementi configurati (gruppo AD, utente o SGT):

- Gruppi e utenti AD: nessuna modifica al comportamento precedente. Il criterio viene confrontato se l'utente è un membro del gruppo OPPURE se l'utente è specificato nel criterio.
- Gruppi e utenti SGT e AD: il criterio viene confrontato se l'utente è associato al SGT AND è un membro del gruppo AD, OPPURE se l'utente è specificato nel criterio.
- SGT e utenti: il criterio corrisponde se l'utente è associato al SGT o se l'utente è specificato nel criterio.

Tra tutti i servizi forniti dall'SWA, la valutazione del traffico HTTPS è la più significativa dal punto di vista delle prestazioni. La percentuale di traffico decrittografato influisce direttamente sulle dimensioni dell'accessorio. Un amministratore può contare su almeno il 75% del traffico Web come HTTPS.

Dopo l'installazione iniziale, è necessario determinare la percentuale di traffico decriptato per garantire che le aspettative di crescita futura siano impostate correttamente. Dopo la distribuzione, questo numero deve essere controllato una volta al trimestre. Trovare la percentuale di traffico HTTPS decrittografato dall'SWA è facile con una copia dei log di accesso, anche senza software aggiuntivo di gestione dei log. Per ottenere questo numero è possibile utilizzare i comandi Simple Bash o PowerShell. Di seguito sono riportati i

passaggi descritti per ogni ambiente:

1. Trovare il numero totale di connessioni HTTPS (sia esplicite che trasparenti):

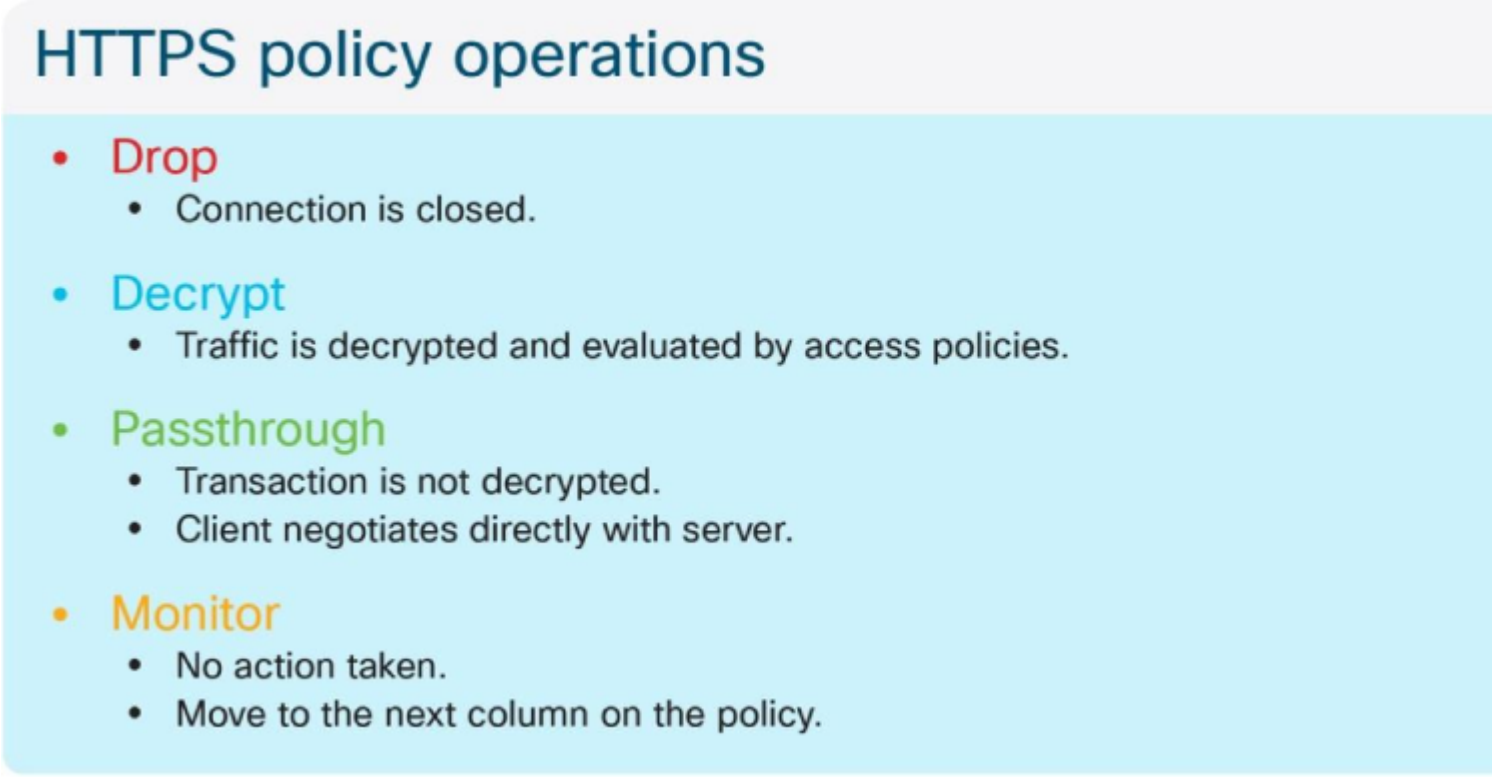
```
Bash:
grep -cE 'tunnel://|TCP_CONNECT' aclog.current

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT').length
```

2. Trovare il numero di connessioni HTTPS decrittografate:

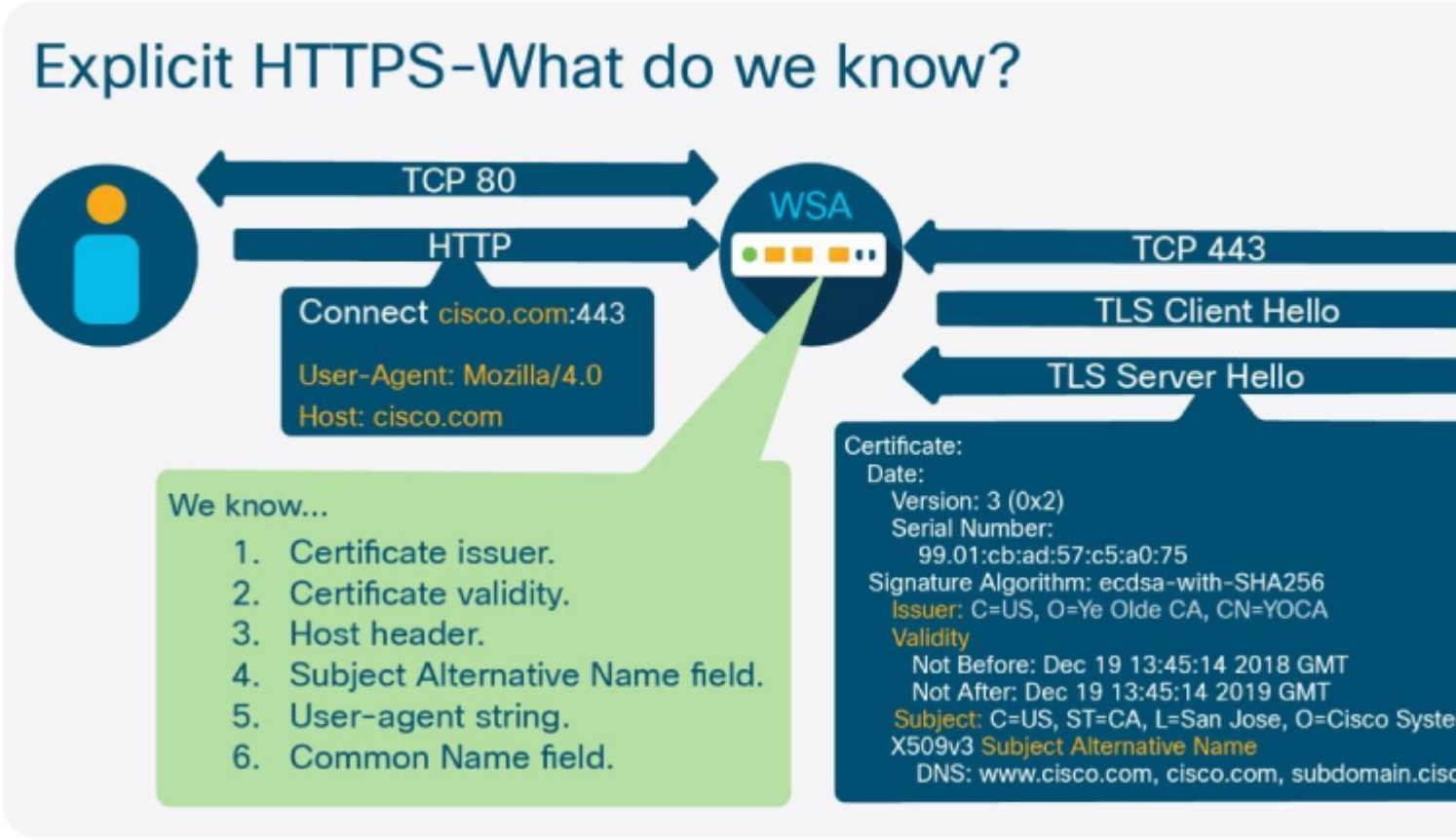
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECTâ€™| Select-String -Pattern â€
```

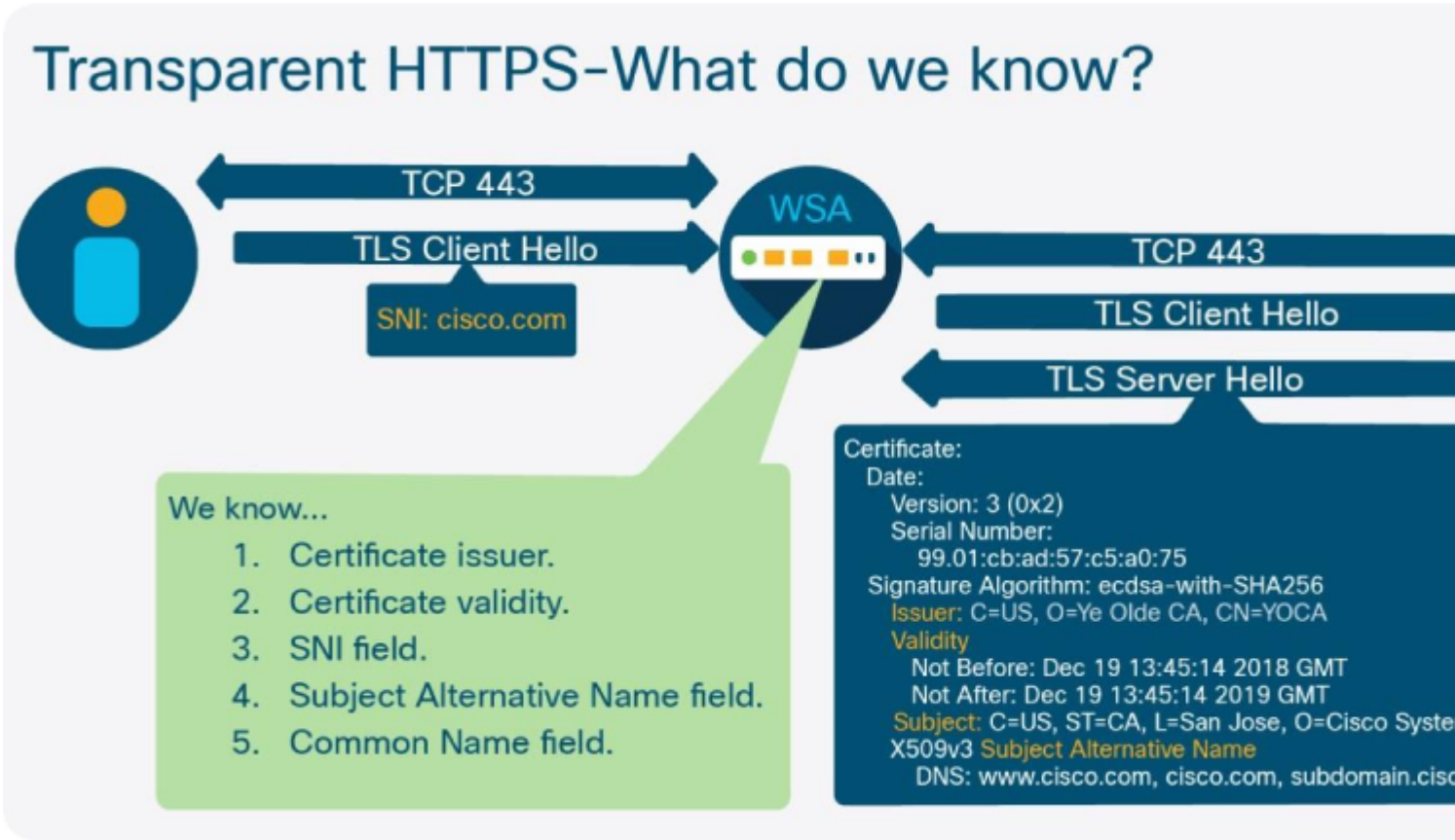
3. Dividere il secondo valore per il primo e moltiplicarlo per 100.

Quando si progettano i criteri di decrittografia, è importante comprendere in che modo le varie azioni elencate nel criterio determinano la valutazione delle connessioni HTTPS da parte dell'accessorio. L'azione passthrough viene usata quando il client e il server devono poter terminare ciascuna estremità della sessione TLS senza che l'SWA decrittografi ogni pacchetto. Anche se un sito è impostato per l'accesso automatico, l'SWA deve comunque completare un handshake TLS con il server. Questo perché l'SWA deve scegliere di bloccare una connessione in base alla validità del certificato e deve avviare una connessione TLS con il server per ottenere il certificato. Se il certificato è valido, l'SWA chiude la connessione e consente al client di continuare a configurare la sessione direttamente con il server.



L'unico caso in cui il SWA non esegue alcun handshake TLS è quando il nome del server o l'indirizzo IP è presente in una categoria personalizzata, impostata su passthrough, e il nome del server è disponibile in HTTP CONNECT o TLS Client Hello. In uno scenario esplicito, il client fornisce il nome host del server al proxy prima dell'avvio della sessione TLS (nell'intestazione host), quindi questo campo viene confrontato con la categoria personalizzata. In una distribuzione trasparente, l'SWA controlla il campo **SNI (Server Name Indication)** nel messaggio Hello del client TLS e lo valuta in base alla categoria personalizzata. Se l'intestazione host o l'SNI non è presente, l'SWA deve continuare l'handshake con il server per controllare i campi **Nome alternativo soggetto (SAN)** e **Nome comune (CN)** sul certificato, nell'ordine indicato. Questo comportamento significa che il numero di handshake TLS può essere ridotto determinando i server noti e considerati internamente attendibili e impostandoli in modo che passino dall'elenco di categorie personalizzato, anziché basarsi sulla categoria Web e sul punteggio di reputazione, che richiedono ancora che l'SWA completi un handshake TLS con il server. È tuttavia importante notare che ciò impedisce anche i controlli di validità dei certificati.





La velocità con cui i nuovi siti vengono visualizzati sul Web, è probabile che un certo numero di siti non siano classificati in base ai database di reputazione Web e di categorizzazioni utilizzati dal SWA. Ciò non indica che il sito è necessariamente più probabile che sia dannoso, e inoltre tutti questi siti sono ancora soggetti a scansione AV, reputazione e analisi dei file AMP e qualsiasi blocco degli oggetti o scansione che è configurato. Per questi motivi, nella maggior parte dei casi non è consigliabile eliminare i siti non

classificati. È consigliabile impostarli in modo che vengano decriptati e analizzati dai motori A/V e valutati da AVC, AMP, policy di accesso e così via. Per ulteriori informazioni sui siti senza categoria, vedere la sezione **Criteri di accesso**.

Criteri di accesso

Come per il profilo ID, anche i criteri impostati nei criteri di decrittografia vengono valutati come AND logico con un'importante eccezione quando vengono utilizzate informazioni provenienti dall'ISE. Di seguito viene descritto il comportamento della corrispondenza ai criteri, in base agli elementi configurati (gruppo AD, utente o SGT):

- Gruppi e utenti di Active Directory: nessuna modifica al comportamento precedente. Il criterio corrisponde se l'utente è un membro del gruppo OPPURE se l'utente è specificato nel criterio.
- Gruppi e utenti SGT e AD: il criterio corrisponde se l'utente è associato a SGT AND è un membro del gruppo AD, OPPURE se l'utente è specificato nel criterio.
- SGT e utenti: il criterio corrisponde se l'utente è associato al SGT OPPURE se l'utente è specificato nel criterio.

Il traffico HTTP viene valutato in base ai criteri di accesso subito dopo l'autenticazione. Il traffico HTTPS viene valutato dopo l'autenticazione e se l'azione di decrittografia viene applicata in base al criterio di decrittografia corrispondente. Per le richieste decrittografate, sono disponibili due voci access_log. La prima voce di log mostra l'azione applicata alla connessione TLS iniziale (decrittografia), mentre la seconda voce mostra l'azione applicata dal criterio di accesso alla richiesta HTTP decrittografata.
Come spiegato nella sezione **Proxy Web,** le intestazioni di richiesta degli intervalli vengono utilizzate per richiedere uno specifico intervallo di byte di un file e sono comunemente utilizzate dal sistema operativo e dai servizi di aggiornamento delle applicazioni. Per impostazione predefinita, l'SWA rimuove queste intestazioni dalle richieste in uscita, in quanto senza l'intero file non è possibile eseguire la scansione antimalware o utilizzare le funzioni AVC. Se molti host della rete richiedono frequentemente intervalli di byte piccoli per recuperare gli aggiornamenti, ciò può indurre l'SWA a scaricare l'intero file più volte contemporaneamente. In questo modo è possibile esaurire rapidamente la larghezza di banda disponibile su Internet e causare interruzioni del servizio. Le cause più comuni di questo scenario di errore sono i daemon di aggiornamento software e di Microsoft Windows.
Per attenuare questo problema, la soluzione migliore è indirizzare il traffico intorno alla SWA. Ciò non è sempre possibile per gli ambienti distribuiti in modo trasparente e, in questi casi, la soluzione migliore consiste nel creare criteri di accesso dedicati per il traffico e abilitare l'inoltro dell'intestazione delle richieste di intervallo su tali criteri. Si deve considerare che la scansione AV e AVC non sono possibili per queste richieste, quindi le policy devono essere attentamente progettate per indirizzare solo il traffico previsto. Il modo migliore per ottenere questo risultato consiste spesso nell'abbinare la stringa agente utente trovata nell'intestazione della richiesta. La stringa agente utente per i daemon di aggiornamento comuni può essere trovata online oppure le richieste possono essere acquisite da un amministratore ed esaminate. La maggior parte dei servizi di aggiornamento, inclusi gli aggiornamenti software di Microsoft Windows e Adobe, non utilizza HTTPS.
Come descritto nella sezione **Criteri di decrittografia**, non è consigliabile eliminare i siti non classificati nei criteri di decrittografia. Per gli stessi motivi, non è consigliabile bloccarli nei criteri di accesso. Il motore di analisi del contenuto dinamico (DCA) può utilizzare il contenuto di un determinato sito, insieme ad altri dati euristici, per i siti categorizzati che altrimenti verrebbero contrassegnati come non categorizzati dalle ricerche nel database URL. L'attivazione di questa funzione riduce il numero di verdetti non classificati nell'SWA.
Nelle impostazioni di Object Scanning di un criterio di accesso è possibile esaminare diversi tipi di file di archivio. Se la rete scarica regolarmente i file di archivio come parte degli aggiornamenti dell'applicazione, l'attivazione di questa opzione può aumentare notevolmente l'utilizzo della CPU. Questo traffico deve essere identificato in anticipo ed esentato se l'intenzione è quella di ispezionare tutti i file di archivio. La prima posizione in cui esaminare i possibili metodi per identificare questo traffico è la stringa agente utente, in quanto ciò può aiutare a evitare gli elenchi IP consentiti che possono diventare difficili da mantenere.

Categorie di URL personalizzati ed esterni

Gli elenchi di categorie personalizzati vengono utilizzati per identificare un server in base all'indirizzo IP o al nome host. È possibile utilizzare le espressioni regolari (regex) per specificare i modelli in base ai quali è possibile trovare una corrispondenza tra i nomi dei server. L'utilizzo di un modello regex per la corrispondenza di un nome di server richiede un impiego di risorse molto più intenso rispetto all'utilizzo di una corrispondenza di sottostringa e pertanto tali modelli devono essere utilizzati solo in caso di assoluta necessità. È possibile aggiungere un "." all'inizio di un nome di dominio in modo che corrisponda a un sottodominio senza la necessità di regex. Ad esempio, ".cisco.com" corrisponde anche a "www.cisco.com".
Come illustrato nella sezione **Complessità**, per complessità ridotta si intendono dieci elenchi di categorie personalizzate, complessità media venti e complessità elevata trenta. Si consiglia di mantenere questo numero al di sotto di venti, soprattutto se gli elenchi utilizzano modelli regex o contengono un numero elevato di voci. Fare riferimento alla sezione **Criteri di accesso** per ulteriori dettagli sul numero di voci per ciascun tipo.
I feed URL esterni sono molto più flessibili degli elenchi di categorie personalizzati statici e il loro utilizzo può avere un impatto diretto sulla sicurezza in quanto rende superflua la gestione manuale da parte di un amministratore. Poiché questa funzione può essere utilizzata per recuperare elenchi non gestiti o controllati dall'amministratore SWA, la possibilità di aggiungere singole eccezioni agli indirizzi scaricati è stata aggiunta in AsyncOS versione 11.8.
L'API di Office365 è particolarmente utile per prendere decisioni su questo servizio comunemente implementato e può essere utilizzata per singole applicazioni (PowerPoint, Skype, Word e così via). Microsoft consiglia di ignorare i proxy per tutto il traffico di Office 365 per ottimizzare le prestazioni. Nella documentazione Microsoft è indicato quanto segue:
"Mentre SSL Break and Inspect crea la latenza più grande, altri servizi, quali l'autenticazione proxy e la ricerca della reputazione, possono causare prestazioni scadenti e un'esperienza utente inadeguata. Inoltre, questi dispositivi di rete perimetrale necessitano di capacità sufficiente per elaborare tutte le richieste di connessione di rete. È consigliabile ignorare il proxy o i dispositivi di ispezione per le richieste di rete dirette di Office 365."https://learn.microsoft.com/en-us/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide .

Può essere difficile utilizzare queste linee guida in un ambiente proxy trasparente. A partire dalla versione 11.8 di AsyncOS, è possibile utilizzare l'elenco delle categorie dinamiche recuperato dall'API di Office365 per popolare l'elenco delle impostazioni di bypass. Questo elenco viene usato per inviare il traffico reindirizzato in modo trasparente al dispositivo WCCP per il routing diretto.
Ignorare tutto il traffico di Office 365 crea un angolo morto per gli amministratori che richiedono alcuni controlli di sicurezza di base e la creazione di rapporti per questo traffico. Se il traffico di Office365 non viene ignorato dall'autorità di certificazione SWA, è importante comprendere le problematiche tecniche specifiche che possono verificarsi. Uno di questi è il numero di connessioni richieste dalle applicazioni. Il ridimensionamento deve essere regolato in modo appropriato per supportare le ulteriori connessioni TCP permanenti richieste dalle applicazioni di Office365. In questo modo è possibile aumentare il numero totale di connessioni di un numero compreso tra dieci e quindici sessioni TCP permanenti per utente.
Le azioni di decrittografia e ricrittografia eseguite dal proxy HTTPS introducono una piccola latenza nelle connessioni. Le applicazioni Office365 possono essere molto sensibili alla latenza e se altri fattori, come la connessione WAN lenta e la disparità di posizione geografica, complicano questa situazione, l'esperienza dell'utente potrebbe risentirne.
Alcune applicazioni di Office 365 utilizzano parametri TLS proprietari che impediscono al proxy HTTPS di completare un handshake con il server applicazioni. Questa operazione è necessaria per convalidare il certificato o recuperare il nome host. Quando questo è combinato con un'applicazione come Skype for Business che non invia un campo **SNI (Server Name Indication)** nel suo messaggio TLS Client Hello, diventa necessario ignorare completamente questo traffico. AsyncOS 11.8 ha introdotto la possibilità di ignorare il traffico basato solo sull'indirizzo IP di destinazione, senza controlli dei certificati per risolvere questo scenario.

Monitoraggi e avvisi

Monitor CLI

La CLI SWA fornisce comandi per il monitoraggio in tempo reale dei processi importanti. I comandi più utili sono quelli che mostrano le statistiche relative al processo proxy. Il comando **status detail** è una valida fonte per il riepilogo delle metriche relative all'utilizzo delle risorse e alle prestazioni, che include i valori di uptime, larghezza di banda utilizzata, latenza di risposta, numero di connessioni e altro ancora. di seguito è riportato l'output di esempio di questo comando:

```
SWA_CLI>  status detail

Status as of:                  Fri Nov 11 14:06:52 2022 +03
Up since:                      Fri Apr 08 10:15:00 2022 +03 (217d 3h 51m 52s)
System Resource Utilization:
  CPU                                3.3%
  RAM                                6.2%
  Reporting/Logging Disk            45.6%
Transactions per Second:
  Average in last minute               55
  Maximum in last hour                201
  Average in last hour                 65
  Maximum since proxy restart        1031
  Average since proxy restart          51
Bandwidth (Mbps):
  Average in last minute            4.676
  Maximum in last hour            327.258
  Average in last hour             10.845
  Maximum since proxy restart     1581.297
  Average since proxy restart       11.167
Response Time (ms):
  Average in last minute               635
  Maximum in last hour              376209
  Average in last hour                 605
  Maximum since proxy restart      2602943
  Average since proxy restart          701
Cache Hit Rate:
  Average in last minute                 0
  Maximum in last hour                   2
  Average in last hour                   0
  Maximum since proxy restart           15
  Average since proxy restart            0
Connections:
  Idle client connections              186
  Idle server connections              184
  Total client connections            3499
  Total server connections            3632
SSLJobs:
  In queue Avg in last minute            4
  Average in last minute             45214
  SSLInfo Average in last min           94
Network Events:
  Average in last minute               0.0
  Maximum in last minute                35
  Network events in last min        124502
```

Il comando **rate** visualizza in tempo reale informazioni sulla percentuale di CPU utilizzata dal processo proxy, nonché sul numero di richieste al secondo (RPS) e le statistiche della cache. Questo comando continua il polling e la visualizzazione del nuovo output fino a quando non viene interrotto. Questo è un esempio di output del comando:

```
SWA_CLI>  rate

Press Ctrl-C to stop.
  %proxy  reqs                          client    server    %bw  disk  disk
     CPU  /sec   hits blocks misses     kb/sec    kb/sec  saved   wrs   rds
  5.00    51      1    147    370      2283      2268    0.6    48    37
  4.00    36      0    128    237     21695     21687    0.0    47    38
  4.00    48      2    179    307      8168      8154    0.2    65    33
  5.00    53      0    161    372      2894      2880    0.5    48    32
  6.00    52      0    198    328     15110     15100    0.1    63    33
  6.00    77      0    415    363      4695      4684    0.2    48    34
  7.00    85      1    417    433      5270      5251    0.4    49    35
  7.00    67      1    443    228      2242      2232    0.5    85    44
```

Il comando **tcpservices** visualizza le informazioni sulle porte di ascolto dei processi selezionate. Viene inoltre visualizzata una spiegazione di ogni processo e della combinazione di indirizzo e porta:

```
SWA_CLI> tcpservices

System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon

Feature Processes
  coeuslogd    - Main WSA controller
  gui          - GUI process
  hermes       - Mail server for sending alerts, etc.
  java         - Processes for storing and querying Web Tracking data
  musd         - AnyConnect Secure Mobility server
  pacd         - PAC file hosting daemon
  prox         - WSA proxy
  trafmon      - L4 Traffic Monitor
  uds          - User Discovery System (Transparent Auth)
  wccpd        - WCCP daemon

COMMAND      USER         TYPE NODE   NAME
connector    root         IPv4 TCP    127.0.0.1:8823
java         root         IPv6 TCP    [::127.0.0.1]:18081
hybridd      root         IPv4 TCP    127.0.0.1:8833
gui          root         IPv4 TCP    172.16.40.80:8443
ginetd       root         IPv4 TCP    172.16.40.80:ssh
nginx        root         IPv6 TCP    *:4431
nginx        root         IPv4 TCP    127.0.0.1:8843
```

```
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
api_serve    root         IPv4 TCP    172.16.40.80:6080
api_serve    root         IPv4 TCP    127.0.0.1:60001
api_serve    root         IPv4 TCP    172.16.40.80:6443
chimera      root         IPv4 TCP    127.0.0.1:6380
nectar       root         IPv4 TCP    127.0.0.1:6382
redis-ser    root         IPv4 TCP    127.0.0.1:6383
redis-ser    root         IPv4 TCP    127.0.0.1:6379
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25255
prox         root         IPv4 TCP    127.0.0.1:socks
prox         root         IPv6 TCP    [::1]:socks
prox         root         IPv4 TCP    172.16.11.69:socks
prox         root         IPv4 TCP    172.16.11.68:socks
prox         root         IPv4 TCP    172.16.11.252:socks
prox         root         IPv4 TCP    127.0.0.1:ftp-proxy
prox         root         IPv6 TCP    [::1]:ftp-proxy
prox         root         IPv4 TCP    172.16.11.69:ftp-proxy
prox         root         IPv4 TCP    172.16.11.68:ftp-proxy
prox         root         IPv4 TCP    172.16.11.252:ftp-proxy
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
```

```
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25256
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.21.11.69:https
prox         root         IPv4 TCP    172.21.11.68:https
prox         root         IPv4 TCP    172.21.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25257
smart_age    root         IPv6 TCP    [::127.0.0.1]:65501
smart_age    root         IPv6 TCP    [::127.0.0.1]:28073
interface    root         IPv4 TCP    127.0.0.1:domain
stunnel      root         IPv4 TCP    127.0.0.1:32137
```

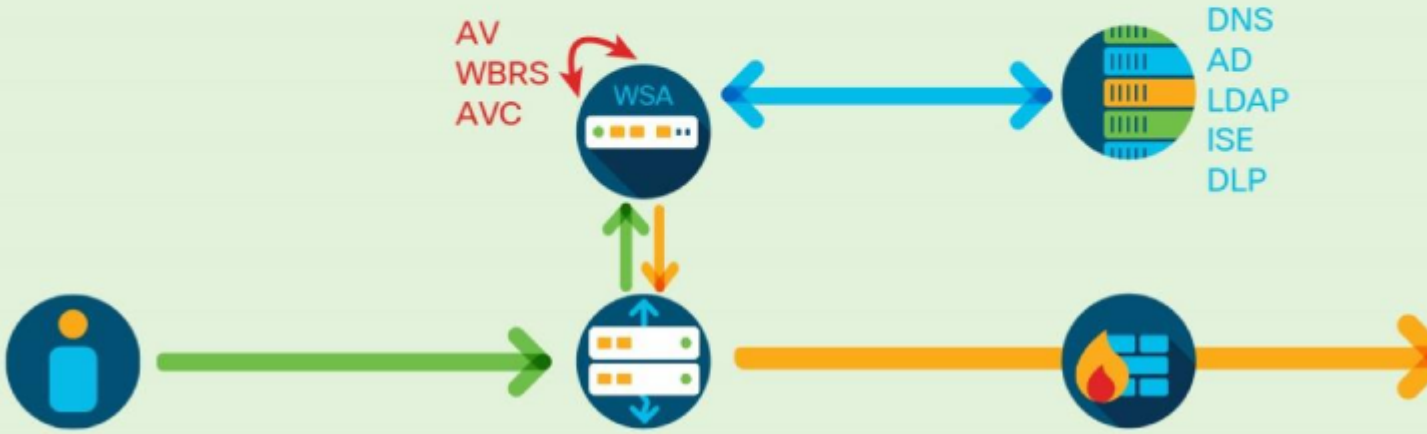
Registrazione

Il traffico Web è estremamente dinamico e vario. Al termine dell'installazione del proxy, è importante riesaminare regolarmente la quantità e la composizione del traffico che attraversa l'accessorio. È necessario controllare regolarmente (una volta al trimestre) la percentuale di traffico decrittografato per verificare che le dimensioni siano conformi alle aspettative e alle specifiche dell'installazione iniziale. A tale scopo, è possibile utilizzare un prodotto per la gestione dei registri, ad esempio **AWSR (Advanced Web Security Reporting)** o comandi semplici Bash o PowerShell con i registri di accesso. Inoltre, il numero di RPS deve essere rivalutato regolarmente per garantire che l'accessorio abbia un sovraccarico sufficiente per tenere conto dei picchi di traffico e del possibile failover in una configurazione ad alta disponibilità con bilanciamento del carico.

Il log track_stats viene aggiunto ogni cinque minuti e include diverse sezioni di output direttamente correlate al processo prox e ai relativi oggetti in memoria. Le sezioni più utili per il monitoraggio delle prestazioni mostrano la latenza media per i vari processi di richiesta, includono il tempo di ricerca DNS, il tempo di scansione del motore AV e molti altri campi utili. Questo registro non è configurabile dalla GUI o dalla CLI ed è accessibile solo tramite SCP (Secure Copy Protocol) o FTP (File Transfer Protocol). Si tratta del registro più importante da avere durante la risoluzione dei problemi relativi alle prestazioni, pertanto deve essere sottoposto a polling frequente.

Where can latency be introduced?

- Client Side
- External Services
- Internal Services
- Server Side

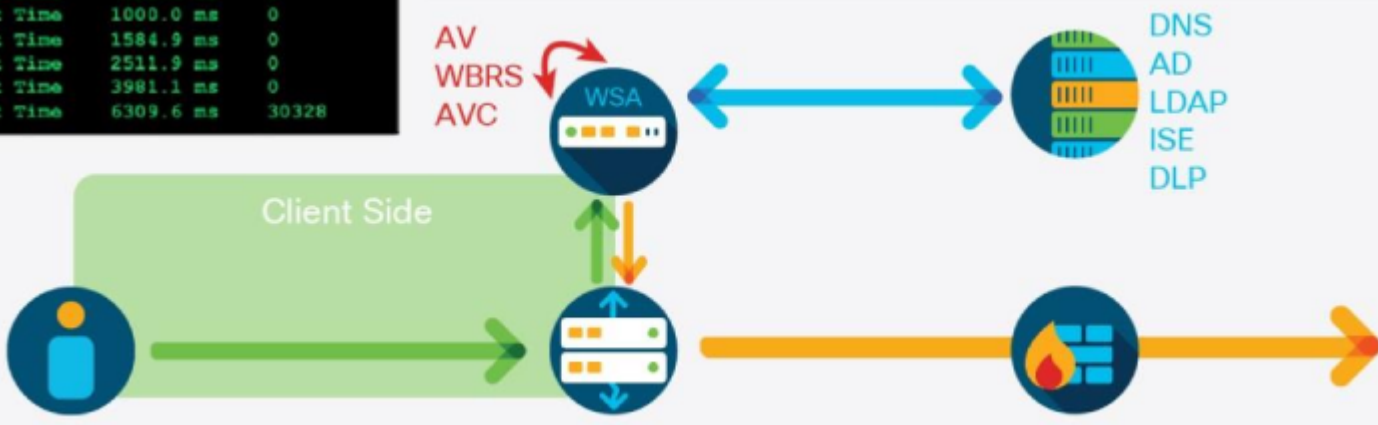


Client side latency

```
Client Time       1.0 ms    15575
Client Time       1.6 ms    185
Client Time       2.5 ms    855
Client Time       4.0 ms    573
Client Time       6.3 ms    180
Client Time      10.0 ms    264
Client Time      15.8 ms    580
Client Time      25.1 ms    924
Client Time      39.8 ms    1330
Client Time      63.1 ms    4936
Client Time     100.0 ms    5278
Client Time     158.5 ms    10
Client Time     251.2 ms    13
Client Time     398.1 ms    0
Client Time     631.0 ms    0
Client Time    1000.0 ms    0
Client Time    1584.9 ms    0
Client Time    2511.9 ms    0
Client Time    3981.1 ms    0
Client Time    6309.6 ms    30328
```

- **“Client Time”** in **track_stats** log.
- The amount of time in milliseconds that the client was wa response.
- May indicate an upstream issues-keep investigating!
- Access logs can show this in custom field **% : 1>**

%:1>	x-p2c-first-byte-time	Wait-time for first byte written

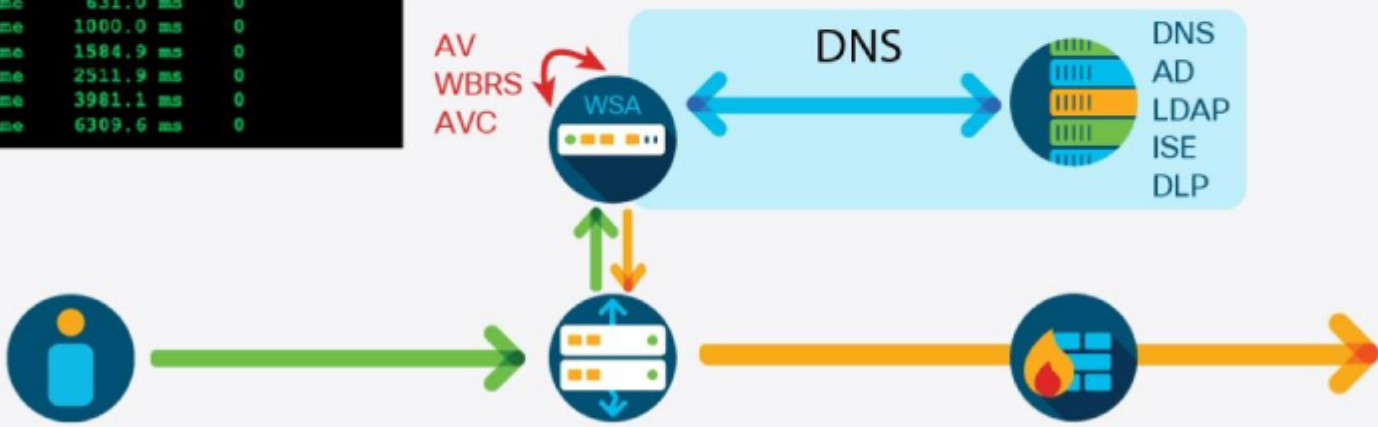


DNS latency

```
DNS Time       1.0 ms    51
DNS Time       1.6 ms    347
DNS Time       2.5 ms    152
DNS Time       4.0 ms    71
DNS Time       6.3 ms    98
DNS Time      10.0 ms    7
DNS Time      15.8 ms    11
DNS Time      25.1 ms    13
DNS Time      39.8 ms    2
DNS Time      63.1 ms    3
DNS Time     100.0 ms    7
DNS Time     158.5 ms    16
DNS Time     251.2 ms    4
DNS Time     398.1 ms    1
DNS Time     631.0 ms    0
DNS Time    1000.0 ms    0
DNS Time    1584.9 ms    0
DNS Time    2511.9 ms    0
DNS Time    3981.1 ms    0
DNS Time    6309.6 ms    0
```

- The amount of time in milliseconds that the WSA waited response.
- Calls for investigation for your DNS resolvers (or path to
- **access logs** can show this in custom field **% : >d**

%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy send a DNS result to ehe Web

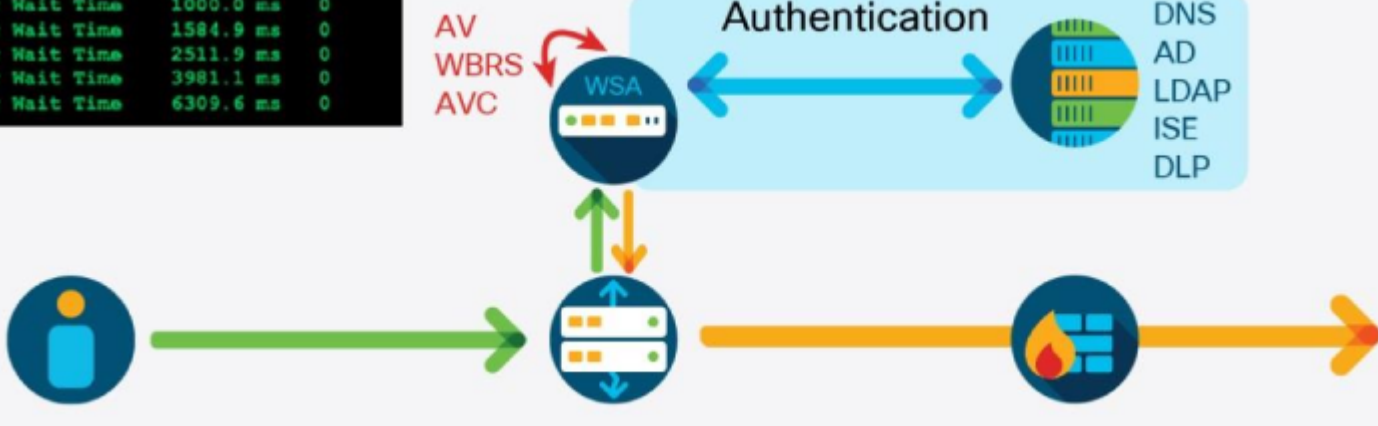


Authentication latency

```
Server Wait Time       1.0 ms    0
Server Wait Time       1.6 ms    0
Server Wait Time       2.5 ms    0
Server Wait Time       4.0 ms    0
Server Wait Time       6.3 ms    0
Server Wait Time      10.0 ms    0
Server Wait Time      15.8 ms    0
Server Wait Time      25.1 ms    0
Server Wait Time      39.8 ms    0
Server Wait Time      63.1 ms    0
Server Wait Time     100.0 ms    0
Server Wait Time     158.5 ms    1
Server Wait Time     251.2 ms    1
Server Wait Time     398.1 ms    0
Server Wait Time     631.0 ms    0
Server Wait Time    1000.0 ms    0
Server Wait Time    1584.9 ms    0
Server Wait Time    2511.9 ms    0
Server Wait Time    3981.1 ms    0
Server Wait Time    6309.6 ms    0
```

- There are two metrics: **“Auth Helper Wait Time”** and **“A Service Wait Time.”**
- Use the first to get pure auth time without the request tim
- **access logs** can show this in custom field **% : >a**

%:<a	x-p2p-auth-wait-time	Wait-time to receive the respo Web Proxy authentication proc Web Proxy sent the request.

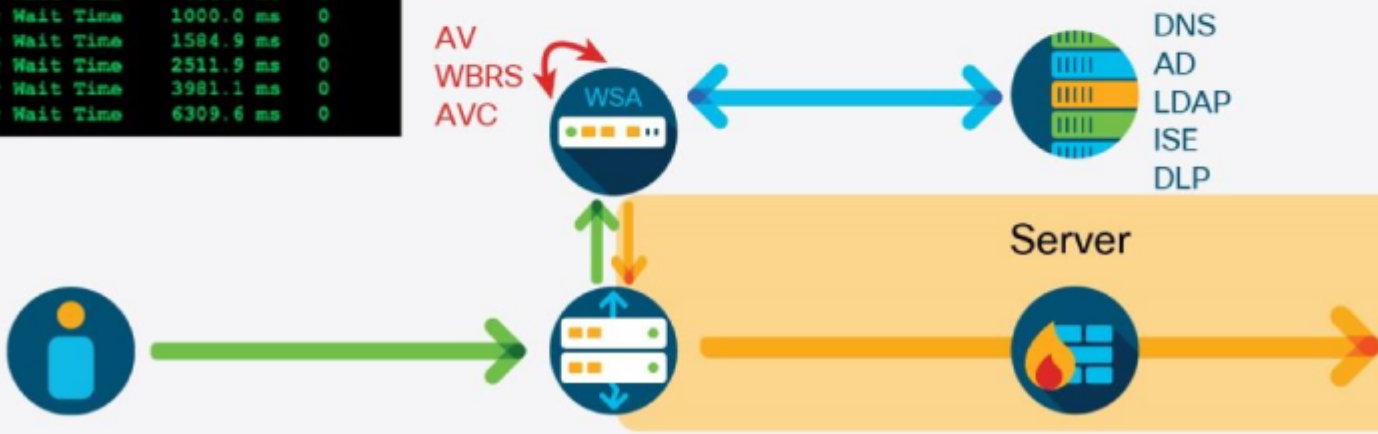


Server latency-wait time

Server Wait Time	1.0 ms	0
Server Wait Time	1.6 ms	0
Server Wait Time	2.5 ms	0
Server Wait Time	4.0 ms	0
Server Wait Time	6.3 ms	0
Server Wait Time	10.0 ms	0
Server Wait Time	15.8 ms	0
Server Wait Time	25.1 ms	0
Server Wait Time	39.8 ms	0
Server Wait Time	63.1 ms	0
Server Wait Time	100.0 ms	0
Server Wait Time	158.5 ms	1
Server Wait Time	251.2 ms	1
Server Wait Time	398.1 ms	0
Server Wait Time	631.0 ms	0
Server Wait Time	1000.0 ms	0
Server Wait Time	1584.9 ms	0
Server Wait Time	2511.9 ms	0
Server Wait Time	3981.1 ms	0
Server Wait Time	6309.6 ms	0

- The amount of time in milliseconds that the WSA waited byte of the server response.
- Calls for investigation of your upstream devices and WAN
- **access logs** can show this in custom field **% : >1**

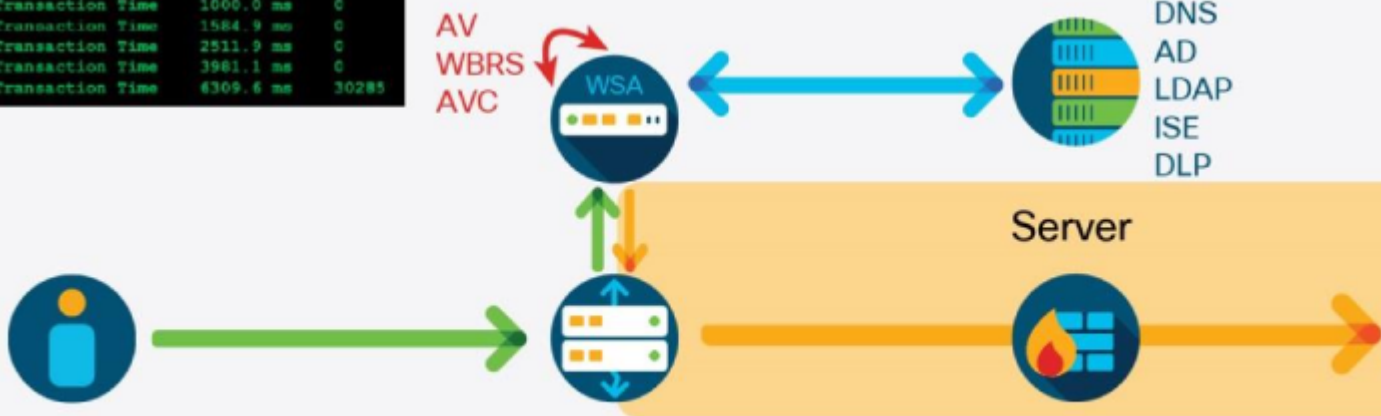
%:>1	x-s2p-first-byte-time	Wait-time for first response by

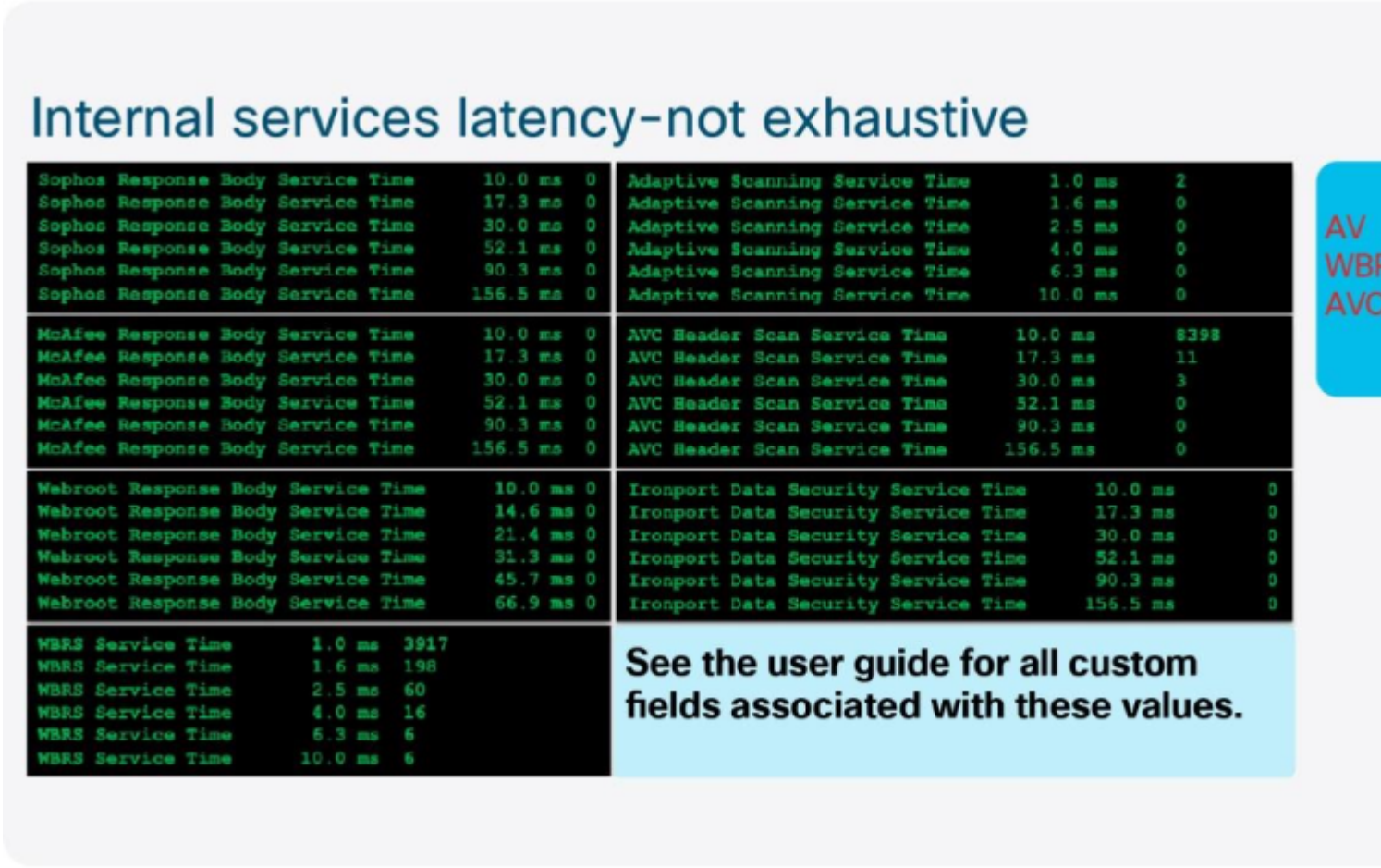


Server latency-transaction time

Server Transaction Time	1.0 ms	1422
Server Transaction Time	1.6 ms	858
Server Transaction Time	2.5 ms	1035
Server Transaction Time	4.0 ms	1106
Server Transaction Time	6.3 ms	758
Server Transaction Time	10.0 ms	810
Server Transaction Time	15.8 ms	288
Server Transaction Time	25.1 ms	45
Server Transaction Time	39.8 ms	73
Server Transaction Time	63.1 ms	4221
Server Transaction Time	100.0 ms	8097
Server Transaction Time	158.5 ms	5
Server Transaction Time	251.2 ms	0
Server Transaction Time	398.1 ms	2
Server Transaction Time	631.0 ms	0
Server Transaction Time	1000.0 ms	0
Server Transaction Time	1584.9 ms	0
Server Transaction Time	2511.9 ms	0
Server Transaction Time	3981.1 ms	0
Server Transaction Time	6309.6 ms	30285

- The amount of time in milliseconds for the entire server-s transaction to complete.
- Calls for investigation of your upstream devices and WAN
- No **access logs** custom field, but can be determined by a combinationof them.





Ogni 60 secondi viene scritta una singola riga di registro SHD contenente molti campi importanti per il monitoraggio delle prestazioni, tra cui latenza, RPS e connessioni client e server totali. Questo è un esempio di una riga di log SHD:

```
Fri Nov 11 14:16:42 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 62 Band 11383 Latency 619
Fri Nov 11 14:17:42 2022 Info: Status: CPULd 2.6 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 10532 Latency 774
Fri Nov 11 14:18:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.6 Reqs 48 Band 7285 Latency 579
Fri Nov 11 14:19:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.6 Reqs 52 Band 34294 Latency 791
Fri Nov 11 14:20:43 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 8696 Latency 691
Fri Nov 11 14:21:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 49 Band 7064 Latency 1403
Fri Nov 11 14:22:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.8 Reqs 41 Band 5444 Latency 788
Fri Nov 11 14:23:43 2022 Info: Status: CPULd 2.2 DskUtil 45.7 RAMUtil 6.8 Reqs 48 Band 6793 Latency 820
Fri Nov 11 14:24:44 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 44 Band 8735 Latency 673
Fri Nov 11 14:25:44 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 53 Band 8338 Latency 731
```

È possibile aggiungere ulteriori campi personalizzati agli access_logs che indicano le informazioni sulla latenza per le singole richieste. Questi campi includono la risposta del server, la risoluzione DNS e la latenza dello scanner AV. È necessario aggiungere i campi al registro per ottenere informazioni utili per la risoluzione dei problemi. Questa è la stringa del campo personalizzato consigliata:

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms):
```

```
, Response Header = %:h>, Client Body = %:b> ] [ Rx Wait Times (in ms): 1st request byte = %:1<, F

 a; DNS response = %:

  d, WBRS response = %:

   r, AVC response = %:A>, AVC total = %:A<, DCA response = %:C>, DCA total = %:C<, McAfee respons

    s, AMP response = %:e>, AMP total = %:e<; Latency = %x; %L ][Client Port = %F, Server IP = %k,
```

Le informazioni sulle prestazioni derivate da questi valori sono le seguenti:

Campo personalizzato	**Descrizione**
%:<a	Tempo di attesa per la ricezione della risposta dal processo di autenticazione del proxy Web, dopo l'invio della richiesta da parte del proxy Web.
%:<b	Tempo di attesa per la scrittura del corpo della richiesta nel server dopo l'intestazione.
%:<d	Tempo di attesa per la ricezione della risposta dal processo DNS del proxy Web, dopo l'invio della richiesta da parte del proxy Web.
%:<h	Tempo di attesa per la scrittura dell'intestazione della richiesta sul server dopo il primo byte.
%:<r	Tempo di attesa per la ricezione della risposta dai filtri della reputazione Web dopo

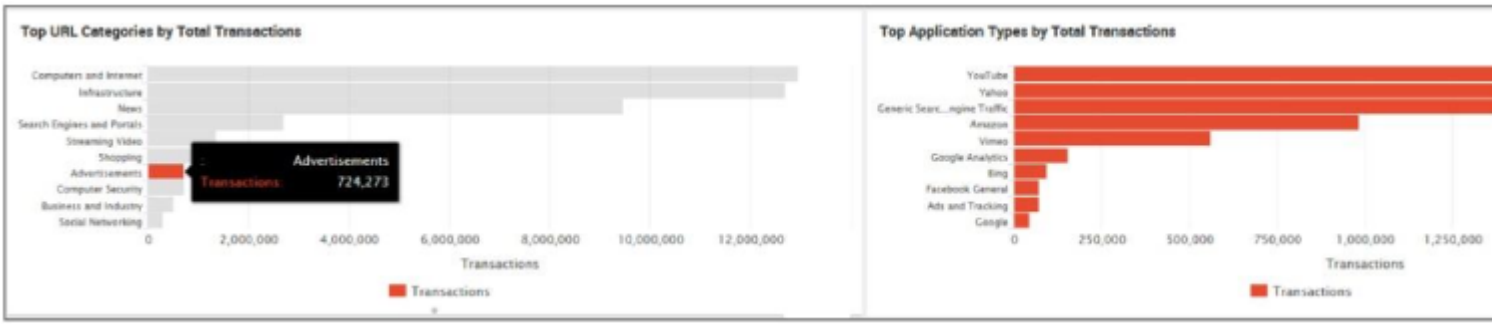
	l'invio della richiesta da parte del proxy Web.
%:<s	Tempo di attesa per la ricezione del verdetto dal processo antispyware del proxy Web, dopo l'invio della richiesta da parte del proxy Web.
%:>	Tempo di attesa per il primo byte di risposta dal server.
%:>a	Tempo di attesa per la ricezione della risposta dal processo di autenticazione del proxy Web, incluso il tempo necessario al proxy Web per inviare la richiesta.
%:>b	Tempo di attesa per il corpo della risposta completo dopo la ricezione dell'intestazione.
%:>c	Tempo necessario al proxy Web per leggere una risposta dalla cache del disco.
%:>d	Tempo di attesa per la ricezione della risposta dal processo DNS del proxy Web, incluso il tempo necessario al proxy Web per inviare la richiesta.
%:>h	Tempo di attesa per l'intestazione del server dopo il primo byte di risposta.
%:>r	Il tempo di attesa per ricevere il verdetto dai filtri della reputazione Web include il tempo necessario al proxy Web per inviare la richiesta.
%:>s	Tempo di attesa per la ricezione del verdetto dal processo antispyware del proxy Web. Include il tempo necessario al proxy Web per inviare la richiesta.
%:1<	Tempo di attesa per il primo byte di richiesta dalla nuova connessione client.
%:1>	Tempo di attesa per il primo byte scritto sul client.
%:b<	Tempo di attesa per il corpo completo del client.
%:b>	Tempo di attesa per il corpo completo scritto sul client.
%:e>	Tempo di attesa per ricevere la risposta dal motore di scansione AMP, dopo l'invio della richiesta da parte del proxy Web.
%:e<	Tempo di attesa per ricevere il verdetto dal motore di scansione AMP, incluso il tempo necessario al proxy Web per inviare la richiesta.
%:h<	Tempo di attesa per l'intestazione client completa dopo il primo byte.
%:h>	Tempo di attesa per la scrittura dell'intestazione completa sul client.
%:m<	Il tempo di attesa per ricevere il verdetto dal motore di scansione McAfee, include il tempo necessario al proxy Web per inviare la richiesta.
%:m>	Tempo di attesa per ricevere la risposta dal motore di scansione McAfee, dopo che il proxy Web ha inviato la richiesta.
%F	Porta di origine del client.
%p	Porta del server Web.
%k	Indirizzo IP origine dati (indirizzo IP server Web).
%:w<	Tempo di attesa per la ricezione del verdetto dal motore di scansione Webroot, incluso il tempo necessario al proxy Web per inviare la richiesta.
%:w>	Tempo di attesa per la ricezione della risposta dal motore di scansione Webroot, dopo l'invio della richiesta da parte del proxy Web.

Il modello di licenza SWA consente di riutilizzare le licenze dei dispositivi fisici per i dispositivi virtuali. È possibile trarre vantaggio da questa situazione e installare accessori SWAv di prova da utilizzare in ambienti di laboratorio. È possibile sperimentare nuove funzionalità e configurazioni in questo modo per garantire

stabilità e affidabilità senza violare, allo stesso tempo, i termini delle licenze.

Advanced Web Security Reporting (AWSR)

L'AWSR deve essere sfruttato per trarre il massimo vantaggio dai dati di reporting provenienti dall'SWA. In particolare, negli ambienti in cui vengono implementati molti SWA, questa soluzione è molto più scalabile rispetto all'utilizzo di report centralizzati su una **Security Management Appliance (SMA)** e fornisce attributi di reporting personalizzati che aggiungono una quantità enorme di profondità e personalizzazione ai dati. I report possono essere raggruppati e personalizzati in base alle esigenze di qualsiasi organizzazione. È necessario utilizzare il gruppo Cisco Advanced Services nel dimensionamento per AWSR.



Avvisi e-mail

Il sistema di allarme via e-mail incorporato nell'SWA è più indicato come sistema di allarme di base. Deve essere modificato in modo appropriato per soddisfare le esigenze dell'amministratore, poiché può essere molto rumoroso se tutti gli eventi informativi sono abilitati. È più importante limitare gli avvisi e monitorarli attivamente che avvisare su tutto e ignorarli come spam.

Impostazioni avvisi	**Configurazione**
Indirizzo mittente da utilizzare per l'invio di avvisi	Generato automaticamente
Numero iniziale di secondi di attesa prima dell'invio di un avviso duplicato	300 secondi
Numero massimo di secondi di attesa prima dell'invio di un avviso duplicato	3600 secondi

Monitoraggio della disponibilità

Esistono due metodi per monitorare la disponibilità di un proxy Web. Il primo è il monitoraggio di **layer 3 (L3)**, che verifica se l'indirizzo IP dell'accessorio è raggiungibile sulla rete. Il modo più semplice per verificare questa condizione è inviare una richiesta **ICMP Echo (ping)** all'indirizzo a intervalli regolari e verificare la presenza di un pacchetto di risposta. È possibile analizzare gli attributi della risposta, ad esempio TTL e latenza, per determinare lo stato del livello di rete.

È possibile che un dispositivo risponda ai ping ma che i processi proxy non rispondano o siano intermittenti. Per questo motivo, è consigliabile utilizzare un monitor di **layer 7 (L7)**, che invia una richiesta proxy esplicita all'accessorio e prevede un codice di risposta HTTP **200 OK**. In questo modo viene verificata non solo la raggiungibilità dell'interfaccia di rete, ma anche la velocità di risposta dei servizi proxy e la fattibilità dei servizi upstream se viene richiesta una risorsa esterna. Questo tipo di monitoraggio in genere assume la forma di una richiesta HTTP **HEAD** esplicita che richiede al proxy di connettersi a una risorsa. Il metodo **HEAD** richiede che le intestazioni che verrebbero restituite devono essere inviate dal client tramite una richiesta **GET**, ma include solo le intestazioni di risposta e nessun dato.

Se si utilizza uno script o uno strumento di monitoraggio **L7**, è importante verificare che il traffico sia escluso dall'autenticazione. In caso contrario, si verificheranno errori di autenticazione e un consumo regolare di risorse. Quando si utilizza una stringa agente utente personalizzata nello strumento di monitoraggio, per identificare il traffico è necessario utilizzare. Anche se il traffico è esentato dall'autenticazione, può comunque essere limitato dall'accesso a Internet non necessario attraverso le policy di accesso.

Quando si utilizza uno o più di questi metodi, un amministratore deve stabilire una baseline di metriche accettabili per la risposta del proxy e utilizzarla per creare le soglie di alert. È necessario dedicare del tempo a raccogliere le risposte di tali controlli e prima di decidere come configurare le soglie e l'avviso.

Monitoraggio SNMP

Il protocollo **SNMP (Simple Network Management Protocol)** è il metodo principale per il monitoraggio dello stato dell'accessorio. Può essere utilizzato per ricevere avvisi dall'accessorio (trap) o per eseguire il polling di vari **identificatori di oggetto (OID, Object Identifier)** per raccogliere informazioni. Nell'SWA sono disponibili molti OID che coprono tutti gli aspetti, dall'hardware all'utilizzo delle risorse, alle informazioni sui singoli processi e alle statistiche sulle richieste.

Esistono diversi **MIB (Machine Information Base)** specifici che devono essere monitorati per motivi legati all'hardware e alle prestazioni. L'elenco completo dei MIB è disponibile qui: https://www.cisco.com/web/ironport/tools/web/asyncosweb-mib.txt.

Questo è un elenco dei MIB consigliati da monitorare e non un elenco esaustivo:

OID hardware	Nome
1.3.6.1.4.1.15497.1.1.1.18.1.3	raidID
1.3.6.1.4.1.15497.1.1.1.18.1.2	statoRAID
1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLastError
1.3.6.1.4.1.15497.1.1.1.10	TabellaVentagli
1.3.6.1.4.1.15497.1.1.1.9.1.2	gradi Celsius

Gli OID vengono mappati direttamente all'output del comando **status detail** CLI:

OID	Nome	Campo Dettaglio stato
Risorse di sistema		
1.3.6.1.4.1.15497.1.1.1.2.0	PercentualeCPUtilizzazione	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	PercentualeUtilizzoMemoria	RAM
Transazioni al secondo		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThroughputOra	Media transazioni al secondo nell'ultimo minuto.

1.3.6.1.4.1.15497.1.2.3.7.1.2.0	CacheThruput1hrPeak	Numero massimo di transazioni al secondo nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMean	Media transazioni al secondo nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	Numero massimo di transazioni al secondo dal riavvio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	DurataThroughputCacheMedia	Numero medio di transazioni al secondo dal riavvio del proxy.
Larghezza di banda		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheLarghezzaBandaTotaleOra	Larghezza di banda media nell'ultimo minuto.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	Larghezza di banda massima nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	Larghezza di banda media nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	Larghezza di banda massima dal riavvio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	Larghezza di banda media dal riavvio del proxy.
Tempo di risposta		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheAccessiOra	Frequenza media riscontri cache nell'ultimo minuto.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	Frequenza massima di accesso alla cache nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	Frequenza media di riscontri nella cache nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	Frequenza massima di accesso alla cache dal riavvio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	Frequenza media di riscontri nella cache dal riavvio del proxy.
Frequenza riscontri cache		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheAccessiOra	Frequenza media riscontri cache nell'ultimo minuto.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	Frequenza massima di accesso alla cache nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	Frequenza media di riscontri nella cache nell'ultima ora.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	Frequenza massima di accesso alla cache dal riavvio del proxy.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	Frequenza media di riscontri nella cache dal riavvio del proxy.
Connessioni		
1.3.6.1.4.1.15497.1.2.3.2.7.0	.CacheClientIdleConns	Connessioni client inattive.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerInattivitàConn	Connessioni server inattive.

1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotaleConn	Totale connessioni client.
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotaleConn	Totale connessioni server.

Conclusioni

Questa guida cerca di descrivere gli aspetti più importanti della configurazione, dell'installazione e del monitoraggio SWA. Come guida di riferimento, il suo obiettivo è quello di fornire informazioni preziose a coloro che volevano garantire l'uso più efficace dell'SWA. Le best practice qui descritte sono importanti per la stabilità, la scalabilità e l'efficacia del dispositivo come strumento di sicurezza. Cerca anche di rimanere una risorsa rilevante e quindi deve essere aggiornato frequentemente per riflettere i cambiamenti negli ambienti di rete e nelle caratteristiche dei prodotti.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).