Use as práticas recomendadas de dispositivos da Web seguros

Contents

Introdução

Este documento descreve as práticas recomendadas para configurar o Cisco Secure Web Appliance (SWA).

Informações de Apoio

Este guia é uma referência para a configuração de práticas recomendadas e aborda muitos aspectos de uma implantação de SWA, incluindo o ambiente de rede suportado, a configuração de políticas, o monitoramento e a solução de problemas. Embora as práticas recomendadas documentadas aqui sejam importantes para que todos os administradores, arquitetos e operadores entendam, elas são apenas diretrizes e devem ser tratadas como tal. Cada rede tem seus próprios requisitos e desafios específicos.

Como um dispositivo de segurança, o SWA interage com a rede de várias maneiras exclusivas. É uma origem e um destino do tráfego da Web. Ele atua ao mesmo tempo que um servidor Web e um cliente Web. No mínimo, ele emprega técnicas de falsificação de endereço IP do servidor e de man-in-the-middle para inspecionar transações HTTPS. Ele também pode falsificar endereços IP de clientes, o que adiciona outra camada de complexidade à implantação e impõe requisitos adicionais à configuração de rede de suporte. Este guia aborda os problemas mais comuns relacionados à configuração do dispositivo de rede relacionado.

A configuração da política SWA tem implicações não apenas para a eficácia e a aplicação da segurança, mas também para o desempenho do dispositivo. Este guia aborda como a complexidade de uma configuração afeta os recursos do sistema. Ele define a complexidade nesse contexto e descreve como minimizá-la no projeto de políticas. Também se presta atenção a recursos específicos e como eles devem ser configurados para aumentar a segurança, a escalabilidade e a eficácia.

A seção Monitoramento e alertas deste documento explica as maneiras mais eficazes de monitorar o dispositivo e também aborda o monitoramento de desempenho e disponibilidade, bem como o uso de recursos do sistema. Ele também fornece informações úteis na solução básica de problemas.

Ambiente de rede

ICMP

Path MTU Discovery, conforme definido no RFC 1191, o mecanismo determina o tamanho máximo de um pacote ao longo de caminhos arbitrários. No caso do IPv4, um dispositivo pode determinar a Unidade Máxima de Transmissão (MTU) de qualquer pacote ao longo de um caminho definindo o bit de Não Fragmentar (DF) no cabeçalho IP do pacote. Se, em algum link ao longo do caminho, um dispositivo não puder encaminhar o pacote sem fragmentá-lo, uma mensagem Internet Control Message Protocol (ICMP) Fragmentation Needed (Type 3, Code 4) será enviada de volta à origem. O cliente então reenvia um pacote menor. Isso continua até que o

MTU do caminho completo seja descoberto. O IPv6 não oferece suporte à fragmentação e usa uma mensagem ICMPv6 de Pacote Muito Grande (Tipo 2) para indicar a incapacidade de ajustar um pacote por meio de um determinado link.

Como o processo de fragmentação de pacotes pode ter impactos graves no desempenho de um fluxo TCP, o SWA utiliza Path MTU Discovery. As mensagens ICMP mencionadas devem ser ativadas em dispositivos de rede relevantes para permitir que o SWA determine o MTU para seu caminho através da rede. Esse comportamento pode ser desabilitado no SWA usando o comando da interface de linha de comando (CLI) pathmtudiscovery. Fazer isso faz com que o MTU padrão caia para 576 bytes (por RFC 879), afetando gravemente o desempenho. O administrador deve executar a etapa adicional de configurar manualmente o MTU no SWA a partir do comando CLI etherconfig.

No caso do Web Cache Communication Protocol (WCCP), o tráfego da Web é redirecionado para o SWA a partir de outro dispositivo de rede ao longo do caminho do cliente para a Internet. Nesse caso, outros protocolos, como o ICMP, não são redirecionados para o SWA. Há uma possibilidade de que o SWA possa disparar uma mensagem ICMP Fragmentation Needed de um roteador na rede, mas a mensagem não seria entregue ao SWA. Se essa for uma possibilidade na rede, a Path MTU Discovery deverá ser desabilitada. Conforme mencionado, com essa configuração, é necessária a etapa adicional de configuração manual da MTU no SWA usando o comando CLI etherconfig.

Firewalls

Em uma configuração padrão, o SWA não falsifica o endereço IP do cliente ao usar proxy em uma conexão. Isso significa que todo o tráfego de saída da Web é originado do endereço IP do SWA. É necessário garantir que os dispositivos Network Address Translation (NAT) tenham um pool grande o suficiente de endereços externos e portas para acomodar isso. É recomendável dedicar um endereço específico para essa finalidade.

Alguns firewalls empregam proteções de negação de serviço (DoS) ou outros recursos de segurança que disparam quando um grande número de conexões simultâneas são originadas de um único endereço IP de cliente. Quando o Spoofing do IP do cliente não está habilitado, o endereço IP SWA deve ser excluído dessas proteções.

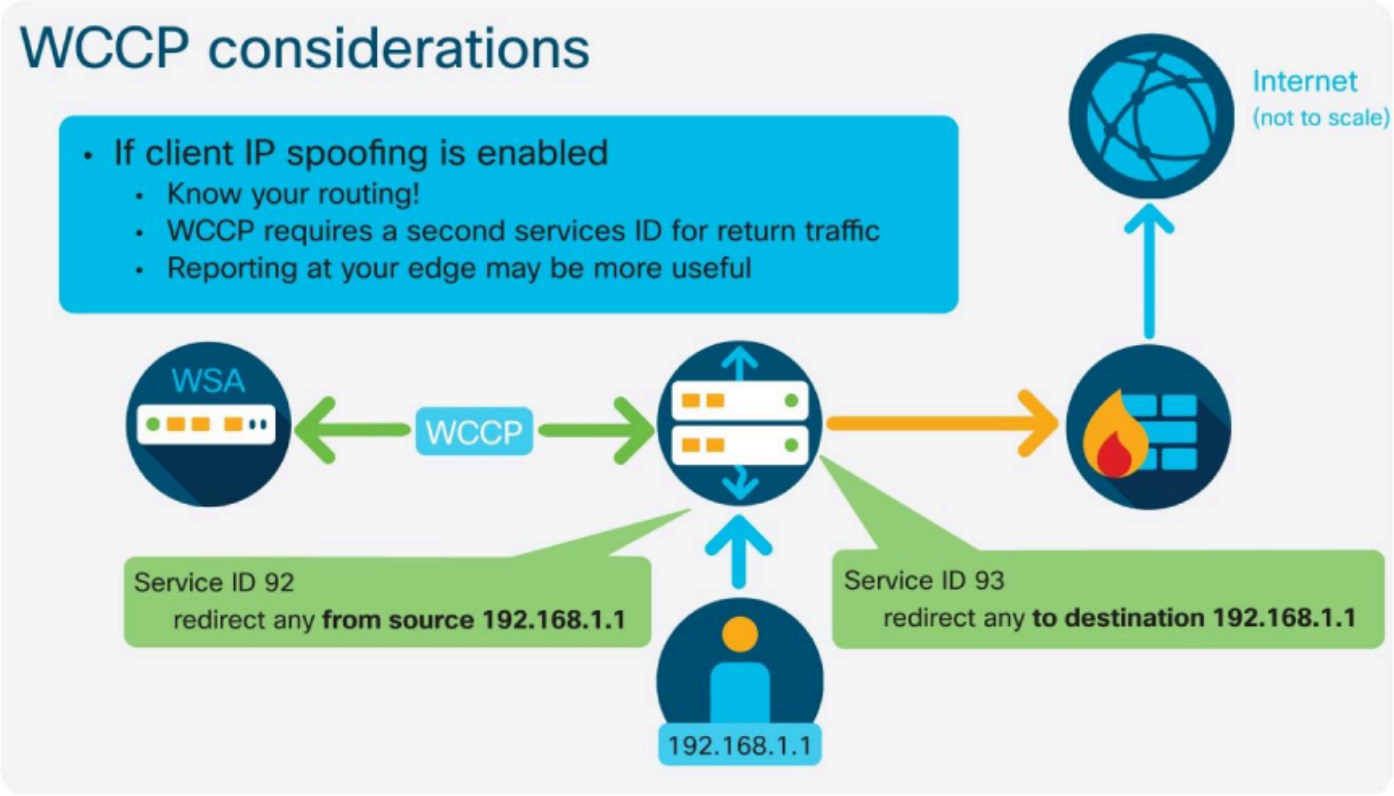
Encaminhamento de caminho reverso unicast

O SWA falsifica o endereço IP do servidor quando se comunica com um cliente e, opcionalmente, pode ser configurado para falsificar o endereço IP do cliente quando se comunica com um servidor upstream. Proteções como Unicast Reverse Path Forwarding (uRPF) podem ser habilitadas nos switches para garantir que um pacote de entrada corresponda à porta de entrada esperada. Essas proteções verificam a interface de origem de um pacote em relação à tabela de roteamento para garantir que ele chegou à porta esperada. Sempre que adequado, os SWA devem ser isentos destas proteções.

Falsificação de IP com WCCP

Quando o recurso IP Spoofing está habilitado no SWA, as solicitações de saída deixam o equipamento e usam o endereço de origem da solicitação do cliente original. Isso exige configuração adicional da infraestrutura de rede relacionada para garantir que os pacotes de retorno sejam roteados para a interface de saída SWA, em vez do cliente que originou a solicitação.

Quando o WCCP é implementado em um dispositivo de rede (roteador, switch ou firewall), é definida uma ID de serviço que corresponde ao tráfego com base em uma ACL (Access Control List, lista de controle de acesso). A ID de serviço é então aplicada a uma interface e usada para corresponder o tráfego para redirecionamento. Se IP Spoofing estiver habilitado, uma segunda ID de serviço deverá ser criada para garantir que o tráfego de retorno também seja redirecionado para o SWA.



Configuração de rede SWA

Interfaces

O SWA tem cinco interfaces de rede utilizáveis: M1, P1, P2, T1 e T2. Cada um deles deve ser aproveitado para seu objetivo específico, quando possível. É vantajoso usar cada porta por suas próprias razões. A interface M1 deve ser conectada a uma rede de gerenciamento dedicada e o roteamento dividido deve ser ativado para limitar a exposição de serviços administrativos. O P1 pode ser limitado ao tráfego de solicitação do cliente. Por outro lado, o P2 não pode aceitar solicitações explícitas de proxy. Isso diminui a quantidade de tráfego em cada interface e permite

uma melhor segmentação no projeto de rede.

As portas T1 e T2 estão disponíveis para o recurso Layer 4 Traffic Monitor (L4TM). Esse recurso monitora uma porta espelhada da camada 2 e adiciona a capacidade de bloquear o tráfego com base em uma lista bloqueada de endereços IP e nomes de domínio mal-intencionados conhecidos. Ele faz isso observando os endereços IP origem e destino do tráfego e envia um pacote de redefinição de TCP, ou mensagem Porta inalcançável se a lista bloqueada for combinada. O tráfego enviado com qualquer protocolo pode ser bloqueado com esse recurso.

Mesmo que o recurso L4TM não esteja habilitado, o desvio transparente pode ser aprimorado quando as portas T1 e T2 estão conectadas a uma porta espelhada. No caso do WCCP, o SWA sabe apenas o endereço IP origem e destino de um pacote recebido e deve tomar a decisão de proxy ou de desvio com base nessas informações. O SWA resolve todas as entradas na lista de configurações de desvio a cada 30 minutos, independentemente do Time to Live (TTL) do registro. No entanto, se o recurso L4TM estiver habilitado, o SWA poderá usar consultas DNS espionadas para atualizar esses registros com mais frequência. Isso reduz o risco de um falso negativo em um cenário onde o cliente resolveu um endereço diferente do SWA.

Roteamento de rede de gerenciamento

Se a rede de gerenciamento dedicada não tiver acesso à Internet, cada serviço poderá ser configurado para usar a tabela de roteamento de dados. Isso pode ser adaptado para se ajustar à topologia de rede, mas, em geral, é recomendável usar a rede de gerenciamento para todos os serviços do sistema e a rede de dados para o tráfego do cliente. A partir da versão 11.0 do AsyncOS, os serviços para os quais o roteamento pode ser definido são:

- Feeds de URL externos
- Reputação e análise de arquivos da AMP (Advanced Malware Protection, proteção avançada contra malware)
- Atualizações e upgrades
- DNS
- Diretório ativo

Para filtragem de saída adicional do tráfego de gerenciamento, os endereços estáticos podem ser configurados para uso nesses serviços:

- Feeds de URL externos:
  1. Personalizado depende de onde eles estão hospedados
  2. Reputação e análise do arquivo AMP
  3. cloud-sa.amp.cisco.com (América do Norte)
  4. cloud-sa.eu.amp.cisco.com (Europa)
  5. cloud-sa.apjc.amp.cisco.com (Ásia-Pacífico)

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

Telemetria TALOS

O grupo Cisco Talos é bem conhecido por identificar ameaças novas e emergentes. Todos os dados enviados ao Talos são anonimizados e armazenados em data centers dos EUA. Participar do SensorBase melhora a categorização e a identificação de ameaças da Web e leva a uma melhor proteção contra o SWA, bem como outras soluções de segurança da Cisco.

DNS

As melhores práticas de segurança do Servidor de Nomes de Domínio (DNS) sugerem que cada rede deve hospedar dois resolvedores de DNS: um para registros autoritativos de um domínio local e outro para resolução recursiva de domínios da Internet. Para acomodar isso, o SWA permite que os servidores DNS sejam configurados para domínios específicos. Se apenas um servidor DNS estiver disponível para consultas locais e recursivas, considere a carga adicional que ele adiciona quando usado para todas as consultas SWA. A melhor opção pode ser usar o resolvedor interno para domínios locais e os resolvedores de Internet raiz para domínios externos. Isso depende do perfil de risco e da tolerância do administrador.

Por padrão, o SWA armazena em cache um registro DNS por no mínimo 30 minutos, independentemente do TTL do registro. Sites modernos que fazem uso intenso de redes de fornecimento de conteúdo (CDNs) têm registros TTL baixos, pois seus endereços IP mudam com frequência. Isso pode fazer com que um cliente armazene em cache um endereço IP para um determinado servidor e o SWA armazene em cache um endereço diferente para o mesmo servidor. Para contornar isso, o TTL padrão do SWA pode ser reduzido para cinco minutos a partir destes comandos 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.
...
```

Os servidores DNS secundários devem ser configurados caso o primário não esteja disponível. Se todos os servidores forem configurados com a mesma prioridade, o IP do servidor será escolhido aleatoriamente. Dependendo do número de servidores configurados, o tempo limite de um determinado servidor pode variar. A tabela é o tempo limite de uma consulta para até seis servidores DNS:

Número de servidores DNS	Tempo limite da consulta (em sequência)

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

Há também opções avançadas de DNS disponíveis apenas através da CLI. Essas opções estão disponíveis na CLI usando o comando advanced proxyconfig > DNS.

Selecione uma destas opções:

- 0 — Sempre usar respostas DNS em ordem
- 1 — Usar o endereço fornecido pelo cliente e depois o DNS
- 2 — Uso limitado de DNS
- 3 — Uso muito limitado do DNS

Para as opções 1 e 2, o DNS será usado se o Web Reputation estiver habilitado.

Para as opções 2 e 3, o DNS é usado para solicitações explícitas de proxy, se não houver proxy de upstream ou se o proxy de upstream configurado falhar.

Para todas as opções, o DNS é usado quando os endereços IP de destino são usados na associação de política.

Essas opções controlam como o SWA decide o endereço IP ao qual se conectar ao avaliar uma solicitação do cliente. Quando uma solicitação é recebida, o SWA vê um endereço IP destino e um nome de host. O SWA deve decidir se confia no endereço IP destino original para a conexão TCP ou fazer sua própria resolução DNS e usar o endereço resolvido. O padrão é "0 = Sempre usar respostas DNS em ordem", o que significa que o SWA não confia no cliente para fornecer o endereço IP.

- Opção 1—O SWA tenta o endereço IP fornecido pelo cliente para a conexão, mas retorna para o endereço resolvido se isso falhar. O endereço resolvido é usado para avaliação de política (categoria da Web, reputação da Web e assim por diante).
- Opção 2—O SWA usa apenas o endereço fornecido pelo cliente para a conexão e não retorna. O endereço resolvido é usado para avaliação de política (categoria da Web, reputação da Web etc.).
- Opção 3—O SWA usa apenas o endereço fornecido pelo cliente para a conexão e não retorna. O endereço IP fornecido pelo cliente é usado para avaliação de política (categoria da Web, reputação da Web etc.).

A opção escolhida depende da confiança que o administrador deve depositar no cliente ao determinar o endereço resolvido para um determinado nome de host. Se o cliente for um proxy de

downstream, escolha a opção 3 para evitar a latência adicional de pesquisas desnecessárias de DNS.

Balanceamento de carga

O WCCP permite o balanceamento transparente de carga de tráfego quando até oito dispositivos são usados. Ele permite o balanceamento de fluxos de tráfego com base em hash ou máscara, pode ser ponderado caso haja uma combinação de modelos de dispositivo na rede e os dispositivos podem ser adicionados e removidos do pool de serviços sem tempo de inatividade. Quando a necessidade exceder o que pode ser tratado com oito SWAs, é recomendável usar um balanceador de carga dedicado.

As melhores práticas específicas para a configuração do WCCP variam de acordo com a plataforma utilizada. Para os switches Cisco Catalyst®, as práticas recomendadas são documentadas no white paper da solução Cisco Catalyst Instant Access .

O WCCP tem limitações quando usado com um Cisco Adaptive Security Appliance (ASA). Ou seja, não há suporte para falsificação de IP do cliente. Além disso, os clientes e SWA devem estar atrás da mesma interface. Por esse motivo, é mais flexível usar um switch ou roteador de camada 4 para redirecionar o tráfego. A configuração do WCCP na plataforma ASA é descrita em WCCP no ASA: Conceitos, Limitações e Configuração.

Para implantações explícitas, um arquivo PAC (Proxy Autoconfiguration) é o método mais amplamente implantado, mas tem muitas desvantagens e implicações de segurança que estão além do escopo deste documento. Se um arquivo PAC for implantado, sugerimos o uso de Objetos de Diretiva de Grupo (GPOs) para configurar o local, em vez de contar com o Protocolo de Descoberta Automática de Proxy da Web (WPAD), que é um alvo comum para invasores e pode ser facilmente explorado se configurado incorretamente. O SWA pode hospedar vários arquivos PAC e controlar sua expiração no cache do navegador.

Um arquivo PAC pode ser solicitado diretamente do SWA de um número de porta TCP configurável (9001 por padrão). Se uma porta não for especificada, a solicitação poderá ser enviada para o próprio processo de proxy como se fosse uma solicitação da Web de saída. Nesse caso, é possível fornecer um arquivo PAC específico com base no cabeçalho do host HTTP presente na solicitação.

O Kerberos deve ser configurado de forma diferente quando usado em um ambiente de alta disponibilidade. O SWA fornece suporte para arquivos keytab, que permite que vários nomes de host sejam associados a um Service Principle Name (SPN). Para obter mais informações, consulte Criação de uma Conta de Serviço no Windows Ative Diretory para Autenticação Kerberos em Implantações de Alta Disponibilidade .

Autenticação ativa

O Kerberos é um protocolo de autenticação mais seguro e amplamente suportado do que o NT LAN Manager Security Support Provider (NTLMSSP). O sistema operacional Apple OS X não oferece suporte a NTLMSSP, mas pode usar Kerberos para autenticar se o domínio tiver ingressado. A autenticação básica não deve ser usada, pois envia credenciais sem criptografia no cabeçalho HTTP e pode ser facilmente detectada por um invasor na rede. Se a autenticação básica precisar ser usada, a criptografia de credenciais deverá ser habilitada para garantir que as credenciais sejam enviadas por um túnel criptografado.

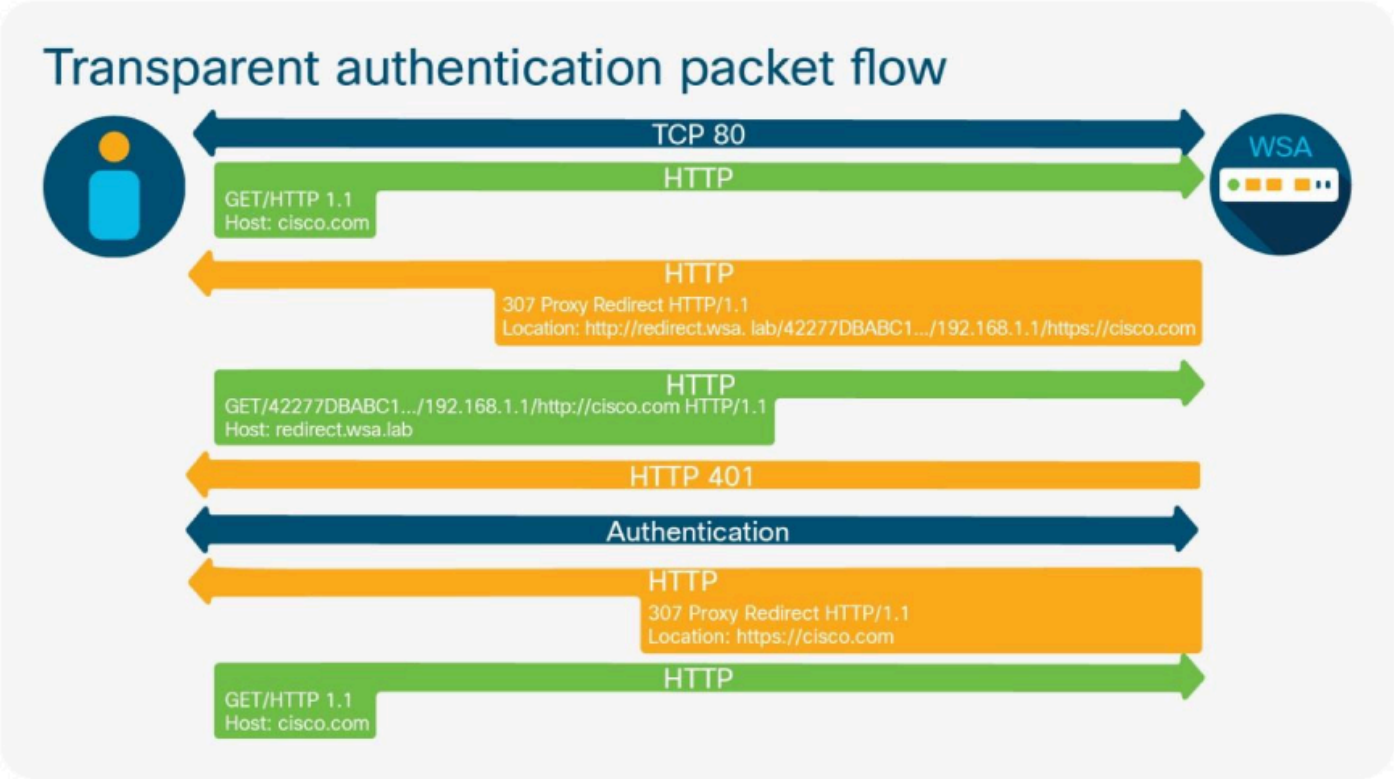
Mais de um controlador de domínio deve ser adicionado à configuração para garantir a disponibilidade, mas não há balanceamento de carga inerente a esse tráfego. O SWA envia um pacote TCP SYN a todos os controladores de domínio configurados e o primeiro a responder é usado para autenticação.

O nome de host de redirecionamento configurado na página de configurações de autenticação determina para onde um cliente transparente é enviado para concluir a autenticação. Para que um cliente Windows conclua a autenticação integrada e obtenha o SSO (Single Sign-On, Logon único), o nome de host de redirecionamento deve estar na zona Sites confiáveis no painel de controle Opções da Internet. O protocolo Kerberos requer que o Fully Qualified Domain Name (FQDN) seja usado para especificar um recurso, o que significa que o "shortname" (ou nome "NETBIOS") não poderá ser usado se Kerberos for o mecanismo de autenticação pretendido. O FQDN precisa ser manualmente adicionado aos Sites Confiáveis (por exemplo, por meio da Política de Grupo). Além disso, o login automático com nome de usuário e senha deve ser definido no painel de controle Opções da Internet.

Também são necessárias configurações adicionais no Firefox para que o navegador conclua a autenticação com proxies de rede. Essas configurações podem ser definidas na página about:config. Para que o Kerberos seja concluído com êxito, o nome de host de redirecionamento deve ser adicionado à opção network.negotiation-auth.trusted-uris. Para NTLMSSP, ele deve ser adicionado à opção network.automatic-ntlm-auth.trusted-uris.

Os substitutos de autenticação são usados para lembrar um usuário autenticado por um período definido após a conclusão da autenticação. Sempre que possível, devem ser usados substitutos de IP para limitar o número de eventos de autenticação ativa que ocorrem. A autenticação ativa de um cliente é uma tarefa que consome muitos recursos, especialmente quando Kerberos é usado. O tempo limite substituto é de 3600 segundos (uma hora) por padrão e pode ser reduzido, mas o menor valor recomendado é de 900 segundos (15 minutos).

Esta imagem mostra como "redirect.WSA.lab" é usado como o nome de host de redirecionamento:



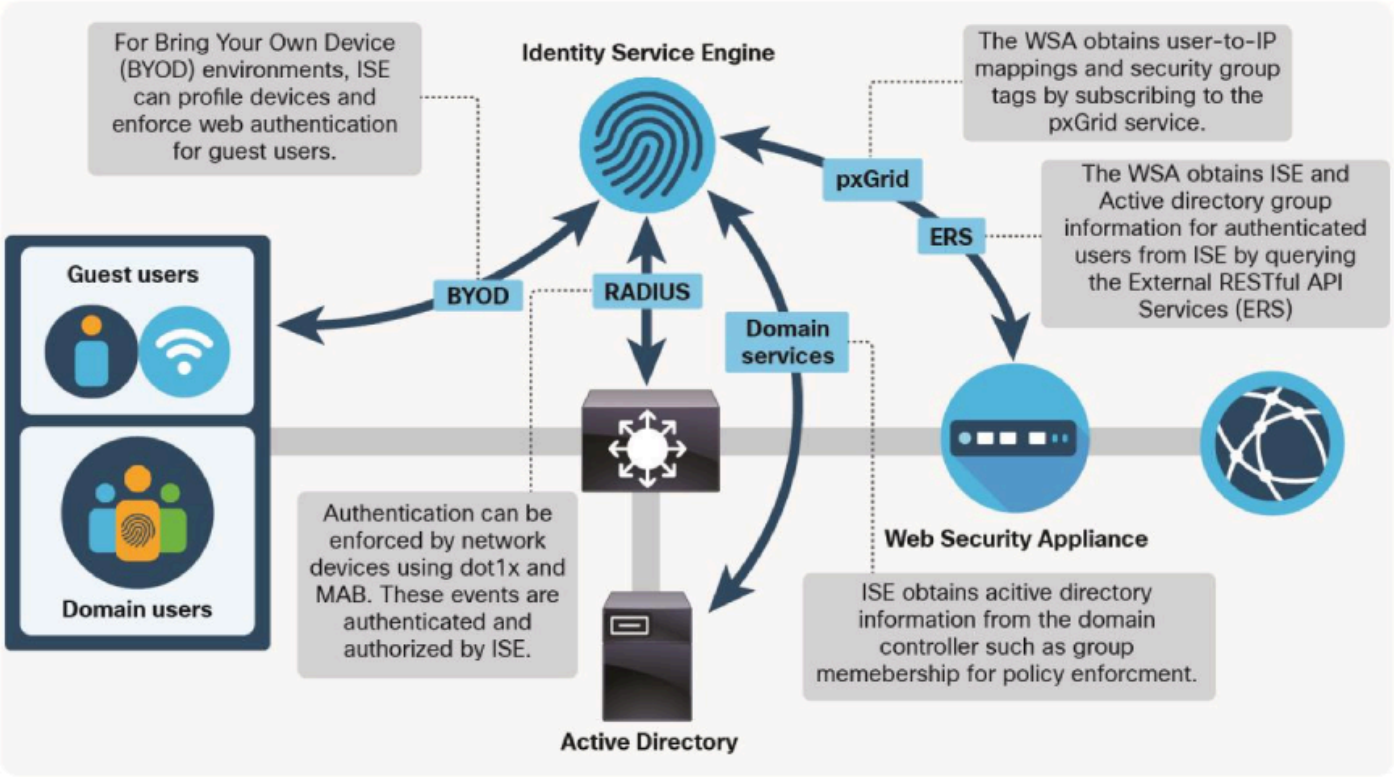
Autenticação Passiva

O SWA pode aproveitar outras plataformas de segurança da Cisco para identificar passivamente usuários proxy. A identificação passiva de usuários elimina a necessidade de um desafio de autenticação direta e qualquer comunicação do Ative Diretory do SWA, o que, por sua vez, reduz a latência e o uso de recursos no dispositivo. Os mecanismos atualmente disponíveis para autenticação passiva são através do Context Diretory Agent (CDA), do Identity Services Engine (ISE) e do Identity Services Connector Passive Identity Connector (ISE-PIC).

O ISE é um produto repleto de recursos que ajuda os administradores a centralizar seus serviços de autenticação e aproveitar um amplo conjunto de controles de acesso à rede. Quando o ISE aprende sobre um evento de autenticação de usuário (por meio da autenticação Dot1x ou do redirecionamento de autenticação da Web), ele preenche um banco de dados de sessão que contém informações sobre o usuário e o dispositivo envolvidos na autenticação. O SWA se conecta ao ISE através do Platform Exchange Grid (pxGrid) e obtém o nome de usuário, o endereço IP e o Security Group Tag (SGT) associados a uma conexão proxy. Desde o AsyncOS versão 11.7, o SWA também pode consultar o Serviço Restful Externo (ERS) no ISE para obter informações de grupo.

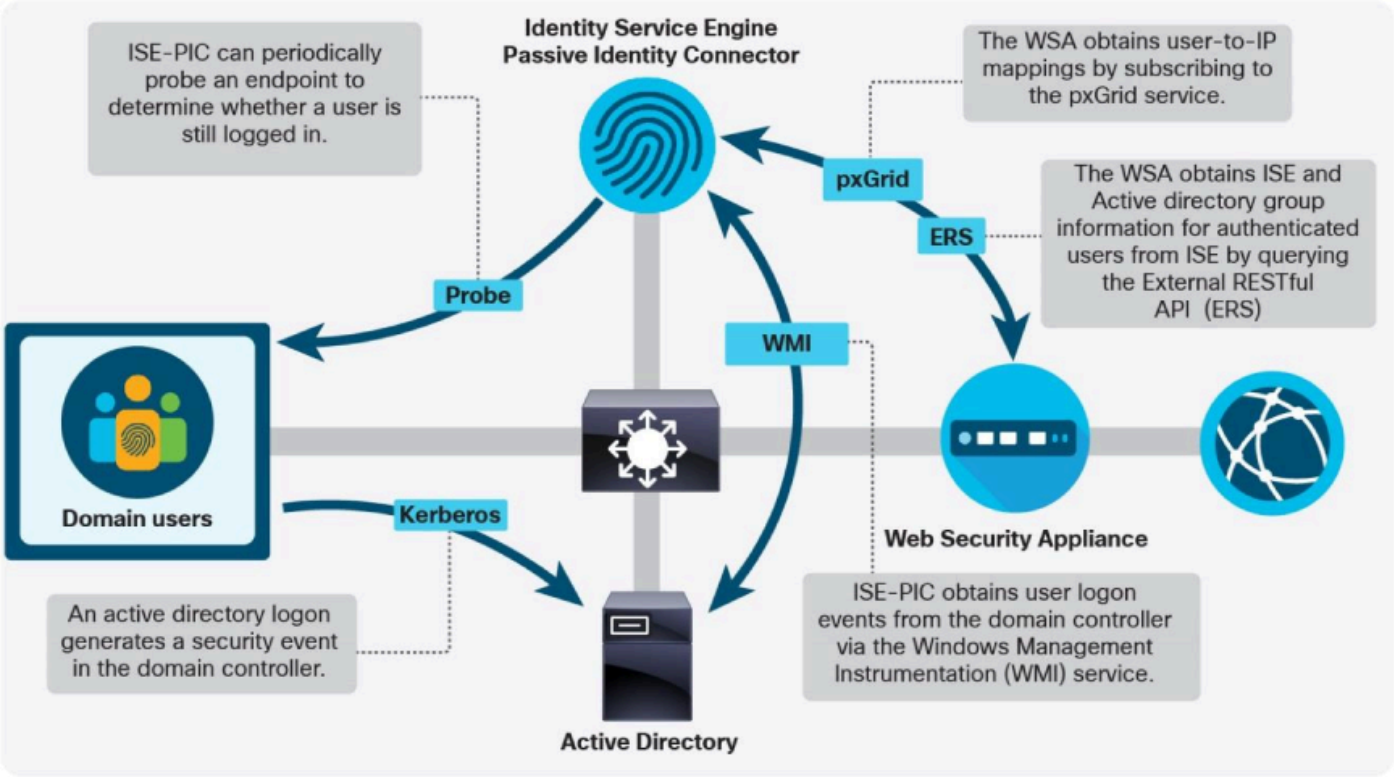
As versões sugeridas são ISE 3.1 e SWA 14.0.2-X e posterior. Para obter mais informações sobre a Matriz de compatibilidade do ISE para SWA, consulte Matriz de compatibilidade do ISE para Secure Web Appliance .

Para obter mais informações sobre etapas de integração completa, consulte Guia do usuário final do Web Security Appliance.



A Cisco anuncia o fim da vida útil do software Cisco Context Diretory Agent (CDA); consulte Cisco Context Diretory Agent (CDA).

A partir do patch 6 do CDA, é compatível com o Microsoft Server 2016. No entanto, os administradores são incentivados ativamente a migrar suas implantações de CDA para ISE-PIC. Ambas as soluções usam o WMI para assinar o Log de Eventos de Segurança do Windows para gerar mapeamentos de usuário para IP (conhecidos como "sessões"). No caso do CDA, o SWA consulta esses mapeamentos com o RADIUS. No caso do ISE-PIC, as mesmas conexões pxGrid e ERS são usadas como na implantação completa do ISE. A funcionalidade ISE-PIC está disponível em uma instalação completa do ISE, bem como em um dispositivo virtual independente.

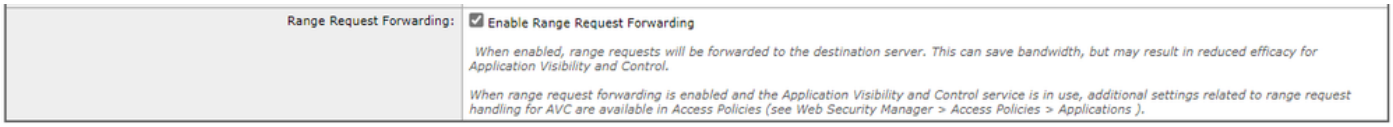


Configuração de serviços

Proxy da Web

O cache deve ser habilitado na configuração do proxy da Web para economizar largura de banda e aumentar o desempenho. Isso está se tornando menos importante à medida que a porcentagem de tráfego HTTPS aumenta, pois o SWA não armazena em cache, por padrão, as transações HTTPS. Se o proxy for implantado para servir apenas clientes explícitos, o modo de encaminhamento deverá ser especificado para rejeitar qualquer tráfego que não seja especificamente destinado ao serviço de proxy. Dessa forma, a superfície de ataque do dispositivo é reduzida e um bom princípio de segurança é praticado: desative-a se não for necessária.

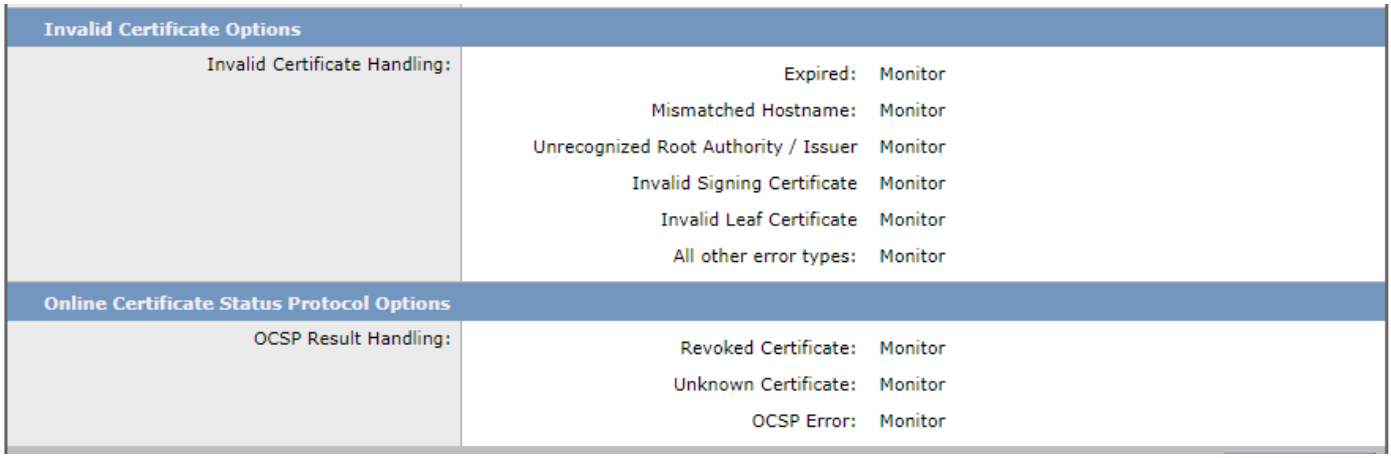
Os cabeçalhos de solicitação de intervalo são usados em solicitações HTTP para especificar o intervalo de bytes de um arquivo a ser baixado. É comumente usado por daemons de atualização de aplicativos e sistemas operacionais para transferir pequenas partes de um arquivo de cada vez. Por padrão, o SWA remove esses cabeçalhos de modo que possa obter o arquivo inteiro para fins de verificação antivírus (AV), reputação e análise de arquivos e Controle de visibilidade de aplicativos (AVC). Habilitar o encaminhamento global de cabeçalhos de solicitação de intervalo nas configurações de proxy permite que os administradores criem políticas de acesso individuais que encaminham ou removem esses cabeçalhos. Mais informações sobre essa configuração são explicadas na seção Access Policies.



Proxy HTTPS

As práticas recomendadas de segurança sugerem que as chaves privadas devem ser geradas no dispositivo onde são usadas e nunca devem ser transportadas para outro lugar. O assistente de proxy HTTPS permite a criação do par de chaves e do certificado usados para descriptografar conexões TLS. A CSR (Certificate Signing Request, solicitação de assinatura de certificado) pode ser baixada e assinada por uma CA (Certificate Authority, autoridade de certificação) interna. Em um ambiente do Ative Diretory (AD), este é o melhor método porque uma CA integrada ao AD é automaticamente confiável para todos os membros do domínio e não requer etapas adicionais para implantar o certificado.

Uma função de segurança do proxy HTTPS é validar certificados de servidor. As práticas recomendadas sugerem que certificados inválidos exigem que a conexão seja descartada. A habilitação de Descriptografar para EUN permite que o SWA apresente uma página de bloqueio explicando o motivo do bloqueio. Sem essa opção habilitada, qualquer site HTTPS bloqueado resultará em um erro de navegador. Isso leva a um aumento nos tíquetes de help desk e a uma suposição por parte do usuário de que algo está quebrado, em vez de saber que o SWA bloqueou a conexão. Todas as opções de certificado inválidas devem ser definidas para pelo menos Descriptografar. Deixar qualquer uma dessas opções como Monitor não poderá registrar mensagens de erro úteis caso problemas de certificado impeçam o carregamento de um site.



Da mesma forma, as verificações do Online Certificate Services Protocol (OCSP) devem ser deixadas habilitadas e o Monitor não deve ser usado para nenhuma opção. Os certificados revogados devem ser descartados e todos os outros devem ser pelo menos definidos como Descriptografar para permitir o registro de mensagens de erro relevantes. A perseguição de acesso a informações de autoridade (AIA chasing) é um meio pelo qual um cliente pode obter o assinante do certificado e uma URL da qual certificados adicionais podem ser buscados. Por exemplo, se uma cadeia de certificados recebida de um servidor estiver incompleta (um certificado intermediário ou raiz está ausente), o SWA poderá verificar o campo AIA e usá-lo para buscar os certificados ausentes e verificar a autenticidade. Essa configuração só está disponível na CLI a partir destes comandos:

```
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]>
...
```

Observação: essa configuração é habilitada por padrão e não deve ser desabilitada, pois muitos servidores modernos dependem desse mecanismo para fornecer uma cadeia de confiança total aos clientes.

Monitor de tráfego de camada 4 (L4TM)

O L4TM é uma maneira altamente eficaz de estender o alcance do SWA para incluir tráfego mal-intencionado que não atravessa o proxy, bem como para incluir o tráfego em todas as portas TCP e UDP. As portas T1 e T2 devem ser conectadas a um toque de rede ou a uma sessão do monitor do switch. Isso permite que o SWA monitore passivamente todo o tráfego dos clientes. Se o tráfego destinado a um endereço IP mal-intencionado for visto, o SWA poderá encerrar sessões TCP enviando um RST enquanto falsifica o endereço IP do servidor. Para o tráfego UDP, ele pode enviar uma mensagem de porta inalcançável. Ao configurar a sessão do monitor, é melhor excluir qualquer tráfego destinado à interface de gerenciamento do SWA para evitar que o recurso interfira potencialmente no acesso ao dispositivo.

Além de monitorar o tráfego mal-intencionado, o L4TM também rastreia consultas DNS para atualizar a lista de configurações de desvio. Essa lista é usada em implantações de WCCP para retornar determinadas solicitações de volta ao roteador WCCP para roteamento direto ao servidor Web. Os pacotes que correspondem à lista de configurações de bypass não são processados pelo proxy. A lista pode conter endereços IP ou nomes de servidor. O SWA resolve todas as entradas na lista de configurações de desvio a cada 30 minutos, independentemente do TTL do registro. No entanto, se o recurso L4TM estiver habilitado, o SWA poderá usar consultas DNS espionadas para atualizar esses registros com mais frequência. Isso reduz o risco de um falso negativo em um cenário onde o cliente resolveu um endereço diferente do SWA.

Configuração de política

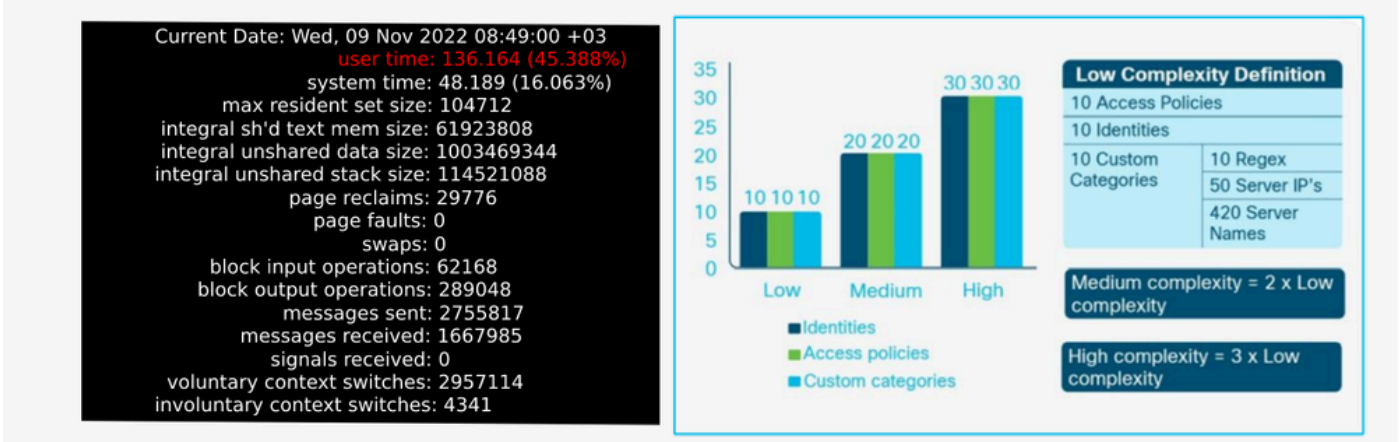
A configuração correta da política é fundamental para o desempenho e a escalabilidade do SWA. Isso é verdade não apenas devido à eficácia das políticas em si na proteção dos clientes e na aplicação dos requisitos da empresa, mas também porque quais políticas são configuradas têm um impacto direto no uso de recursos e na integridade geral e no desempenho do SWA. Um conjunto de políticas excessivamente complexo ou mal projetado pode causar instabilidade e diminuir a capacidade de resposta do dispositivo.

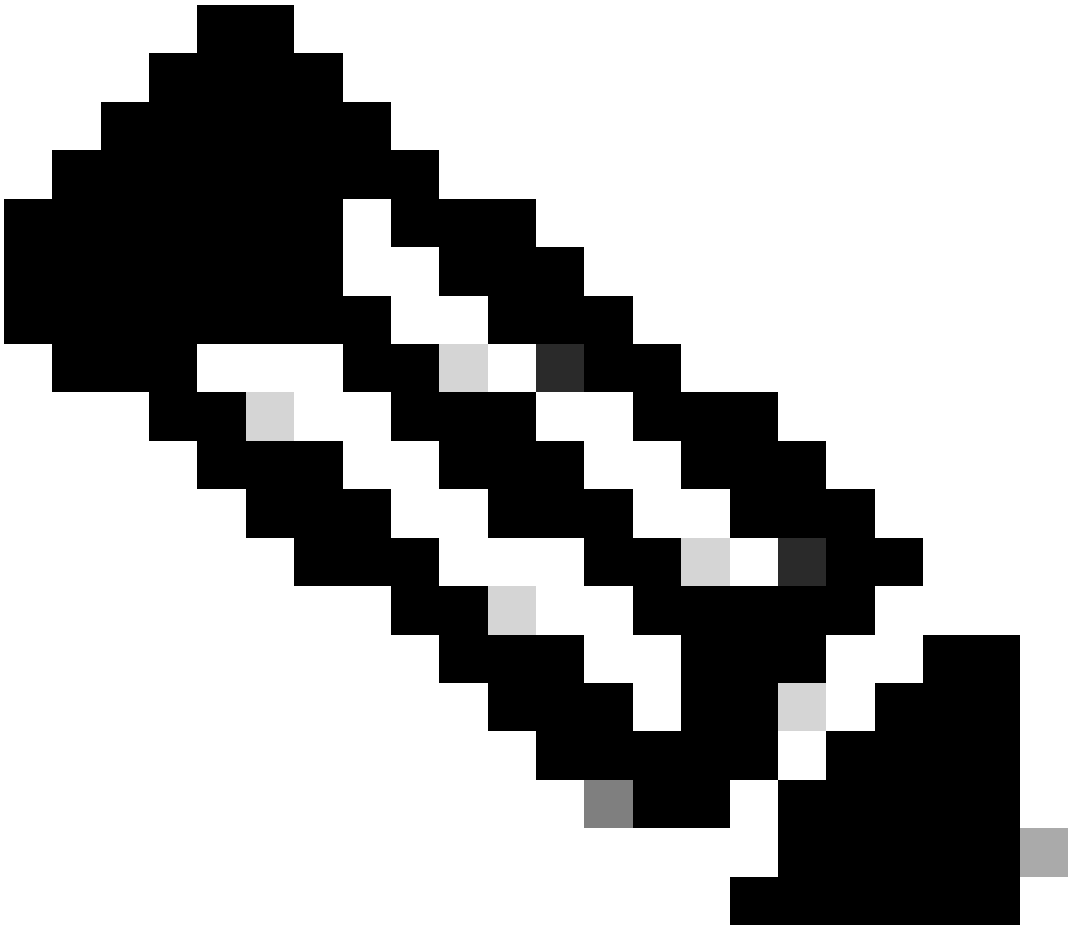
Complexidade

Vários elementos de política são usados na construção de políticas de SWA. O arquivo XML gerado a partir da configuração é usado para criar vários arquivos de configuração de back-end e regras de acesso. Quanto mais complexa for a configuração, mais tempo o processo de proxy terá para avaliar os vários conjuntos de regras para cada transação. Na avaliação comparativa e no dimensionamento do SWA, é criado um conjunto básico de elementos de política que representam três níveis de complexidade de configuração. Dez perfis de identidade, políticas de decodificação e políticas de acesso, juntamente com dez categorias personalizadas contendo dez entradas regex, cinquenta endereços IP de servidor e 420 nomes de host de servidor, são considerados uma configuração de Baixa Complexidade. A multiplicação de cada uma dessas figuras por duas e três resulta em uma configuração de complexidade média e alta complexidade, respectivamente.

Quando uma configuração se torna muito complexa, os primeiros sintomas geralmente incluem uma resposta lenta na interface da Web e na CLI. No início, não pode haver um impacto significativo para os usuários. Mas quanto mais complexa for a configuração, mais tempo o processo proxy deverá passar no modo usuário. Por causa disso, verificar a porcentagem de tempo gasto neste modo pode ser uma maneira útil de diagnosticar uma configuração excessivamente complexa como a causa de um SWA lento.

O tempo de CPU, em segundos, é registrado no registro track_stats a cada cinco minutos. Isso significa que o percentual de tempo do usuário pode ser calculado como (tempo do usuário + tempo do sistema)/300. À medida que o tempo do usuário se aproxima de 270, o processo está gastando muitos ciclos da CPU no modo do usuário, e isso ocorre quase sempre porque a configuração é muito complexa para ser analisada de forma eficiente.





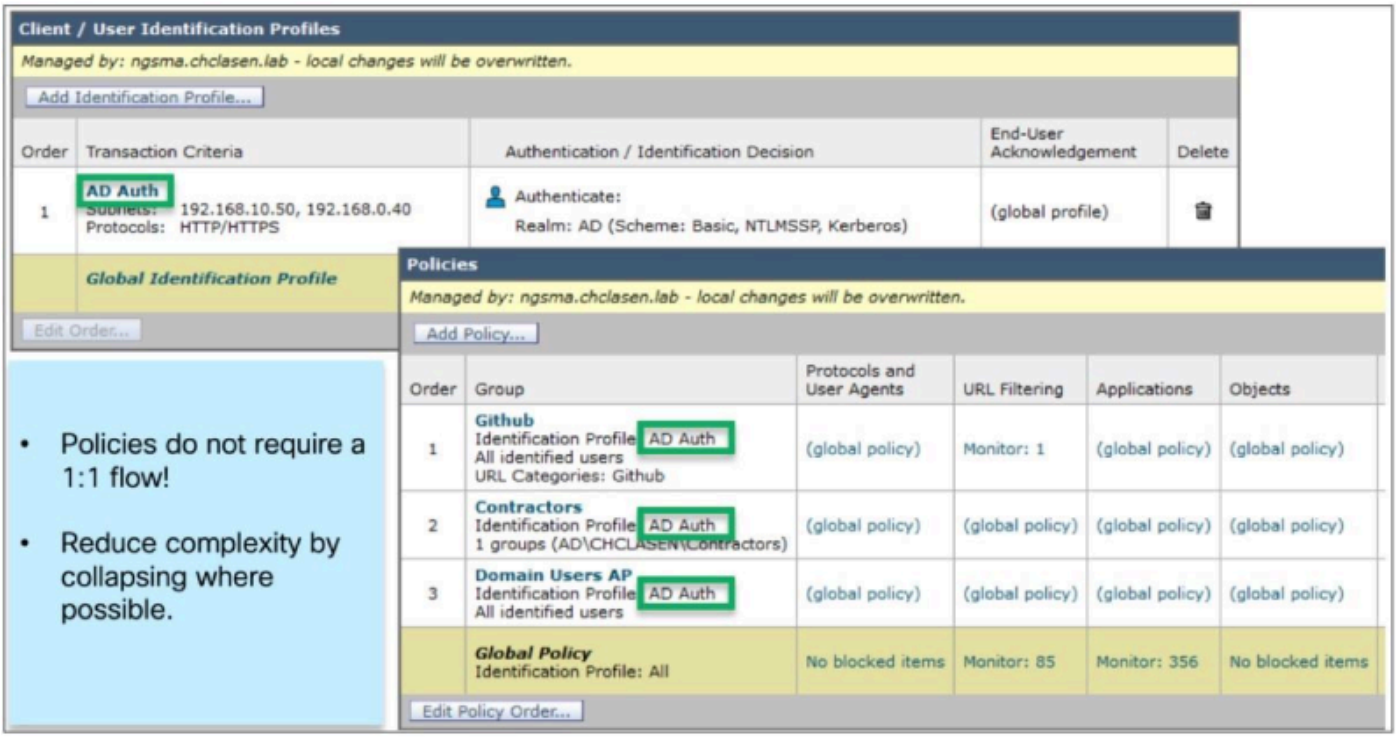
Observação: até o momento, o SWA tem o limite máximo de 60.000 conexões de clientes simultâneas e 60.000 conexões de servidores simultâneos.

Perfis de identificação

Os perfis de Identificação (ID) são os primeiros elementos de política que são avaliados quando uma nova solicitação é recebida. Todas as informações configuradas na primeira seção do perfil de ID são avaliadas com um AND lógico. Isso significa que todos os critérios devem corresponder para que a solicitação corresponda ao perfil. Ao criar uma política, ela deve ser tão específica quanto absolutamente necessário. Os perfis que incluem endereços de host individuais quase nunca são necessários e podem levar a configurações dispersas. Aproveitar a cadeia de caracteres usuário-agente encontrada nos cabeçalhos HTTP, na lista de categorias personalizadas ou na sub-rede é geralmente uma estratégia melhor para limitar o escopo de um perfil.

Em geral, as políticas que exigem autenticação são configuradas na parte inferior e exceções são adicionadas a elas. Ao solicitar políticas que não exigem autenticação, as políticas mais usadas devem estar o mais perto possível do topo. Não confie na falha de autenticação para restringir o acesso. Se um cliente na rede for conhecido por não conseguir se autenticar em um proxy, ele deverá ser isento de autenticação e bloqueado nas políticas de acesso. Os clientes que não podem se autenticar enviam repetidamente solicitações não autenticadas ao SWA, que usam recursos e podem causar utilização excessiva de CPU e memória.

Uma concepção equivocada comum para administradores é que deve haver um perfil de ID exclusivo e a política de descriptografia e de acesso correspondentes. Essa é uma estratégia ineficiente para a configuração de políticas. Quando possível, as políticas devem ser "recolhidas" para que um único perfil de ID possa ser associado a várias políticas de acesso e descriptografia. Isso é possível porque todos os critérios em uma determinada política devem corresponder para que o tráfego corresponda à política. Ser mais geral na política de autenticação e mais específico nas políticas resultantes permite menos políticas como um todo.



Políticas de descriptografia

Como no perfil de ID, os critérios definidos na política de descriptografia também são avaliados como um AND lógico, com uma exceção importante quando são usadas informações do ISE. Veja como a correspondência de políticas funciona, dependendo dos elementos configurados (grupo AD, usuário ou SGT):

- Grupos e usuários do AD — Sem alteração no comportamento anterior; a política será correspondida se o usuário for membro do grupo OU se o usuário for especificado na política.
- Grupos e usuários SGT e AD — A política será correspondida se o usuário estiver associado ao SGT AND for um membro do grupo AD, OU se o usuário estiver especificado na política.
- SGT e usuários — A política será correspondida se o usuário estiver associado ao SGT ou se o usuário estiver especificado na política.

De todos os serviços executados pelo SWA, a avaliação do tráfego HTTPS é a mais significativa do ponto de vista do desempenho. A porcentagem de tráfego descriptografado tem um impacto direto sobre como o dispositivo deve ser dimensionado. Um administrador pode contar com pelo menos 75% do tráfego da Web para ser HTTPS.

Após a instalação inicial, a porcentagem de tráfego descriptografado deve ser determinada para garantir que as expectativas de crescimento futuro sejam definidas com precisão. Após a implantação, esse número deve ser verificado uma vez por trimestre. Encontrar a porcentagem de tráfego HTTPS que é descriptografada pelo SWA é fácil de fazer com uma cópia dos access_logs, mesmo sem software adicional de gerenciamento de logs. Os comandos Simple Bash ou PowerShell podem ser usados para obter esse número. Estas são as etapas descritas para cada ambiente:

1. Comando Linux:

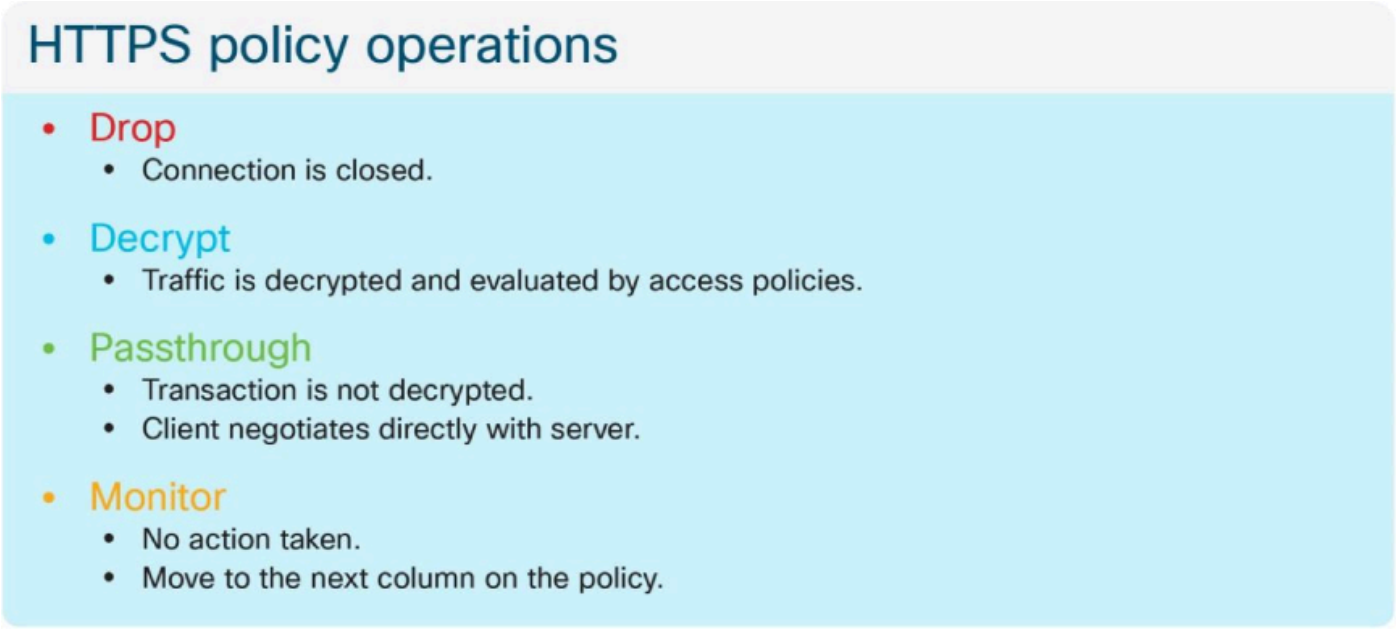
```
cat aclog.current | grep -Ev "\/407|\/401" | awk 'BEGIN { total=0; decrypt=0; ssl=0;} {total++; if($0 ~
```

2. Comando do Powershell:

```
$lines = Get-Content -Path "aclog.current" | Where-Object { $_ -notmatch "/407|/401" }; $total = 0; $de
```

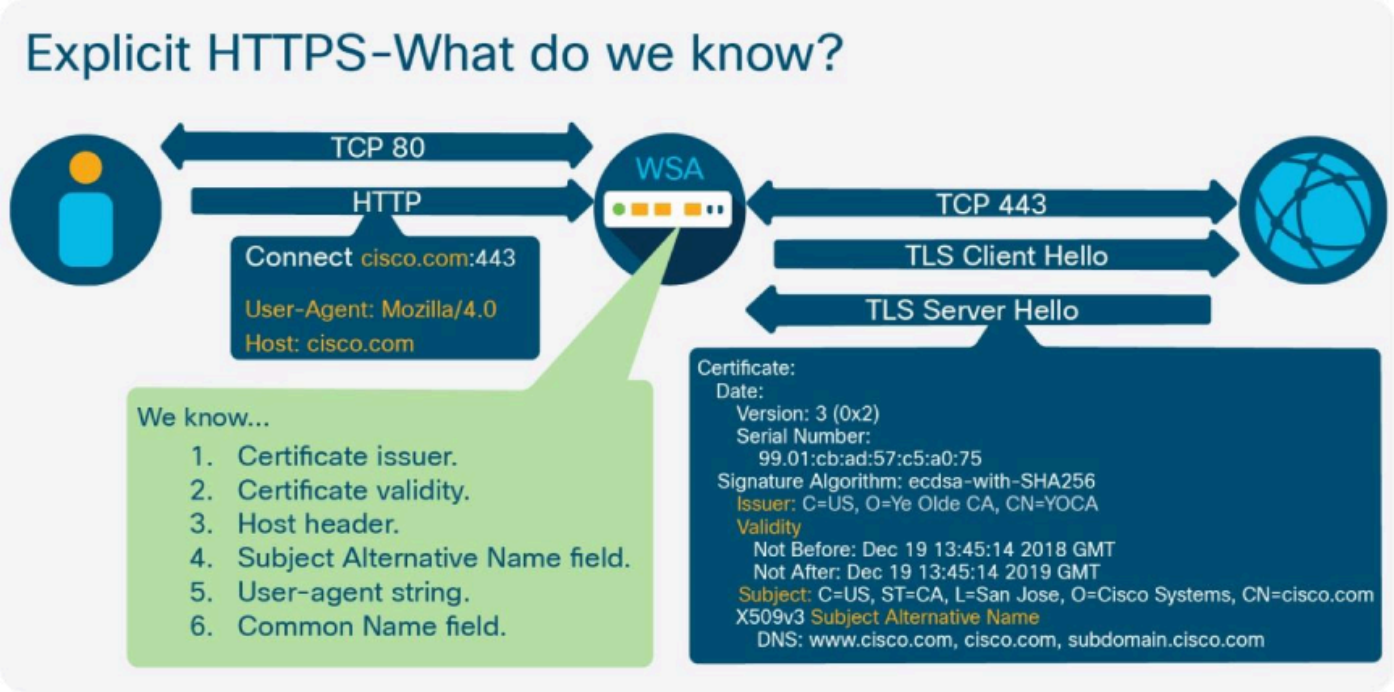
Ao projetar políticas de descriptografia, é importante entender como as várias ações listadas na política fazem com que o equipamento avalie conexões HTTPS. A ação de passagem é usada quando o cliente e o servidor devem ter permissão para terminar cada fim de sua sessão TLS sem que o SWA descriptografe cada pacote. Mesmo que um site esteja configurado para passar, o SWA ainda deverá ser solicitado a concluir um handshake TLS com o servidor. Isso ocorre porque o SWA deve optar por bloquear uma conexão com base na validade do certificado e deve

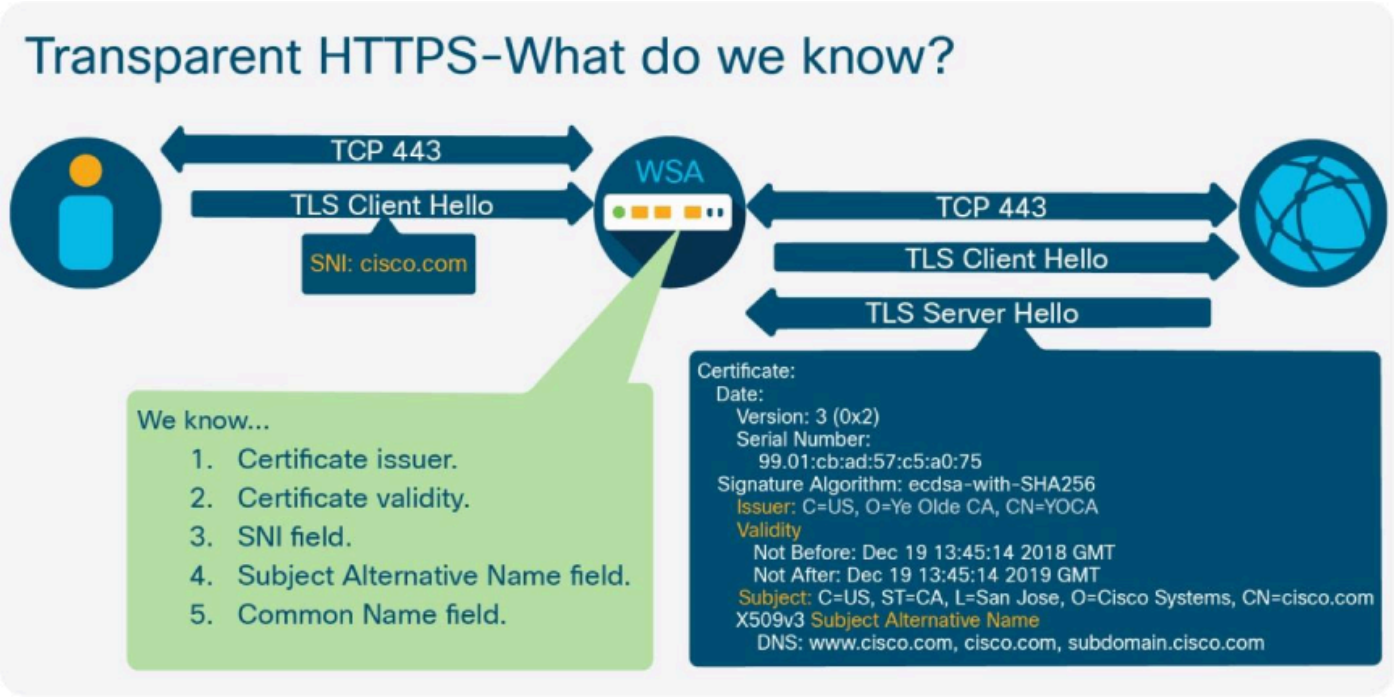
iniciar uma conexão TLS com o servidor para obter o certificado. Se o certificado for válido, o SWA fechará a conexão e permitirá que o cliente continue configurando a sessão diretamente com o servidor.



O único caso em que o SWA não executa nenhum handshake TLS é quando o nome do servidor ou o endereço IP está presente em uma categoria personalizada, que é definida como passagem, e o nome do servidor está disponível em um HTTP CONNECT ou em um TLS Client Hello. Em um cenário explícito, o cliente fornece o nome de host do servidor para o proxy antes do início da sessão TLS (no cabeçalho do host), de modo que este campo é verificado em relação à categoria personalizada. Em uma implantação transparente, o SWA verifica o campo Server Name Indication (SNI) na mensagem de saudação do cliente TLS e o avalia em relação à categoria personalizada. Se o cabeçalho do host ou a SNI não estiver presente, o SWA deverá continuar o handshake com o servidor para verificar os campos Nome alternativo do assunto (SAN) e Nome comum (CN) no certificado, nessa ordem.

O que esse comportamento significa para o design da política é que o número de handshakes de TLS pode ser reduzido determinando servidores conhecidos e internamente confiáveis e definindo-os para passar da lista de categorias personalizadas, em vez de depender da categoria da Web e da pontuação de reputação, que ainda exigem que o SWA conclua um handshake de TLS com o servidor. No entanto, é importante observar que isso também impede verificações de validade do certificado.





Dada a velocidade com que novos sites aparecem na Web, é provável que vários sites sejam encontrados sem categorização pela reputação da Web e pelos bancos de dados de categorização usados pelo SWA. Isso não indica que o site é necessariamente mais propenso a ser mal-intencionado e, além disso, todos esses sites ainda estão sujeitos à verificação de antivírus, à reputação e à análise do arquivo AMP e a qualquer bloqueio ou verificação de objetos configurados. Por esses motivos, não é recomendável descartar sites não categorizados na maioria das circunstâncias. É melhor defini-los para serem descriptografados e examinados pelos mecanismos de antivírus e avaliados pelo AVC, AMP, políticas de acesso, etc. Há mais informações sobre sites não categorizados na seção Políticas de acesso.

Políticas de acesso

Assim como no perfil de ID, os critérios definidos na política de descriptografia também são avaliados como um AND lógico, com uma exceção importante quando são usadas informações do ISE. O comportamento de correspondência de políticas é explicado a seguir, com base nos elementos configurados (grupo AD, usuário ou SGT):

- Grupos e usuários do AD — Sem alteração no comportamento anterior; a política será correspondida se o usuário for membro do grupo OU se o usuário for especificado na política.
- Grupos e usuários SGT e AD — A política será correspondida se o usuário estiver associado ao SGT AND for um membro do grupo AD, OU se o usuário estiver especificado na política.
- SGT e usuários — A política será correspondida se o usuário estiver associado ao SGT OU se o usuário estiver especificado na política.

O tráfego HTTP é avaliado em relação às políticas de acesso imediatamente após ser autenticado. O tráfego HTTPS é avaliado após ser autenticado e se a ação de descriptografia for aplicada de acordo com a política de descriptografia correspondente. Para solicitações descriptografadas, há duas entradas access_log. A primeira entrada de log mostra a ação aplicada à conexão TLS inicial (descriptografar) e uma segunda entrada de log mostra a ação aplicada pela política de acesso à solicitação HTTP descriptografada.

Conforme explicado na seção Web Proxy, os cabeçalhos de solicitação de intervalo são usados para solicitar um intervalo de bytes específico de um arquivo e geralmente são usados pelo SO e pelos serviços de atualização de aplicativos. O SWA, por padrão, retira esses cabeçalhos das solicitações de saída, porque sem o arquivo inteiro, é impossível executar a verificação de malware ou utilizar recursos AVC. Se muitos hosts na rede estiverem solicitando intervalos de bytes pequenos com frequência para recuperar atualizações, isso pode disparar o SWA para baixar o arquivo inteiro várias vezes simultaneamente. Isso pode esgotar rapidamente a largura de banda disponível na Internet e causar interrupções no serviço. As causas mais comuns desse cenário de falha são os daemons de atualização do Microsoft Windows e do software Adobe.

Para atenuar isso, a melhor solução é direcionar todo esse tráfego em torno do SWA. Isso nem sempre é viável para ambientes implantados de forma transparente e, nesses casos, a melhor opção é criar políticas de acesso dedicado para o tráfego e habilitar o encaminhamento de cabeçalho de solicitação de intervalo nessas políticas. Deve-se considerar que a varredura de AV e AVC não é possível para essas solicitações e, portanto, as políticas devem ser cuidadosamente projetadas para direcionar apenas o tráfego pretendido. Frequentemente, a melhor maneira de fazer isso é combinando a string usuário-agente encontrada no cabeçalho da solicitação. A string usuário-agente para daemons de atualização comuns pode ser encontrada on-line ou as solicitações podem ser capturadas por um administrador e examinadas. A maioria dos serviços de atualização, incluindo as atualizações do software Microsoft Windows e Adobe, não usa HTTPS.

Como é descrito na seção Políticas de descriptografia, não é recomendável descartar sites não

categorizados nas políticas de descriptografia. Pelas mesmas razões, não é recomendável bloqueá-los nas políticas de acesso. O mecanismo DCA (Dynamic Content Analysis, análise dinâmica de conteúdo) pode usar o conteúdo de um determinado site, juntamente com outros dados heurísticos, para categorizar sites que, de outra forma, seriam marcados como não categorizados por pesquisas de banco de dados de URL. Habilitar esse recurso reduz o número de vereditos não categorizados no SWA.

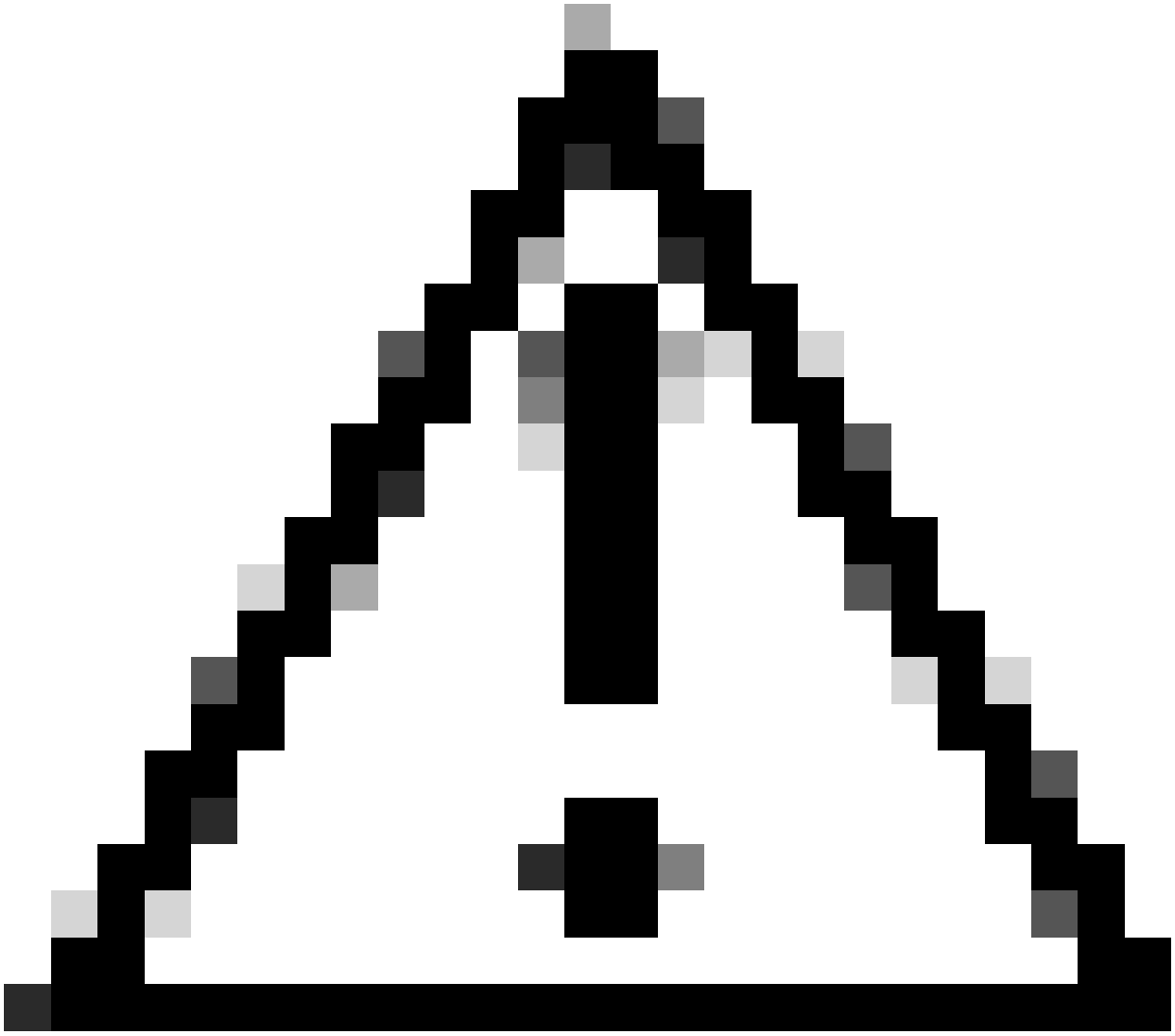
As configurações de Varredura de objetos de uma política de acesso permitem inspecionar vários tipos de arquivos compactados. Se a rede fizer downloads regulares de arquivos como parte das atualizações do aplicativo, a ativação da inspeção de arquivos pode aumentar significativamente o uso da CPU. Esse tráfego deve ser identificado antecipadamente e isento se a intenção for inspecionar todos os arquivos. O primeiro lugar para investigar possíveis métodos para identificar esse tráfego é a string usuário-agente, pois isso pode ajudar a evitar listas de IP permitidas que podem se tornar incômodas para manter.

Categorias de URL personalizadas e externas

As listas de categorias Personalizadas são usadas para identificar um servidor por endereço IP ou nome de host. É possível usar expressões regulares (regex) para especificar padrões pelos quais os nomes de servidor podem ser correspondidos. O uso de um padrão regex para corresponder a um nome de servidor exige muito mais recursos do que o uso de uma correspondência de substring e, portanto, eles só devem ser usados quando absolutamente necessário. Um "." pode ser adicionado ao início de um nome de domínio para corresponder a um subdomínio sem a necessidade de regex. Por exemplo, ".cisco.com" também corresponde a "www.cisco.com".
Conforme explicado na seção Complexidade, baixa complexidade é definida como dez listas de categorias personalizadas, média complexidade como vinte e alta complexidade como trinta. Recomenda-se manter esse número abaixo de vinte, especialmente se as listas usam padrões regex ou contêm um grande número de entradas. Consulte a seção Access Policies para obter detalhes adicionais sobre o número de entradas para cada tipo.

Os feeds de URL externos são muito mais flexíveis do que as listas de categorias personalizadas estáticas, e aproveitá-los pode ter um impacto direto na segurança, pois eliminam a necessidade de um administrador mantê-los manualmente. Como esse recurso pode ser usado para recuperar listas que não são mantidas ou controladas pelo administrador SWA, a capacidade de adicionar exceções individuais aos endereços baixados foi adicionada no AsyncOS versão 11.8.

A API do Office365 é especialmente útil para tomar decisões de política sobre esse serviço normalmente implantado e pode ser aproveitada para aplicativos individuais (PowerPoint, Skype, Word e assim por diante). A Microsoft recomenda ignorar proxies para todo o tráfego do Office365 para otimizar o desempenho. A documentação da Microsoft afirma:



Cuidado: "Enquanto a quebra e inspeção de SSL cria a maior latência, outros serviços, como autenticação de proxy e pesquisa de reputação, podem causar desempenho ruim e uma experiência de usuário ruim. Além disso, esses dispositivos de rede de perímetro precisam de capacidade suficiente para processar todas as solicitações de conexão de rede. Recomendamos que você ignore seus dispositivos proxy ou de inspeção para solicitações diretas de rede do Office 365." - https://learn.microsoft.com/en-us/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide

---

Pode ser difícil usar essa orientação em um ambiente proxy transparente. Começando na versão 11.8 do AsyncOS, é possível usar a lista de categorias dinâmicas recuperada da API do Office365 para preencher a lista de configurações de desvio. Essa lista é usada para enviar o tráfego redirecionado de forma transparente de volta ao dispositivo WCCP para roteamento direto.

Ignorar todo o tráfego do Office365 cria um ponto cego para administradores que exigem alguns controles básicos de segurança e relatórios para esse tráfego. Se o tráfego do Office365 não for ignorado pelo SWA, é importante entender os desafios técnicos específicos que podem surgir.

Um deles é o número de conexões necessárias para os aplicativos. O dimensionamento deve ser ajustado adequadamente para acomodar as conexões TCP persistentes adicionais exigidas pelos aplicativos do Office365. Isso pode aumentar a contagem total de conexões entre dez e quinze sessões TCP persistentes por usuário.

As ações de descriptografia e recriptografia executadas pelo proxy HTTPS apresentam uma pequena quantidade de latência para as conexões. Os aplicativos do Office365 podem ser muito sensíveis à latência e, se outros fatores, como conexão WAN lenta e localização geográfica díspares, o compõem, a experiência do usuário pode ser prejudicada.

Alguns aplicativos do Office365 empregam parâmetros TLS proprietários que impedem que o proxy HTTPS conclua um handshake com o servidor de aplicativos. Isso é necessário para validar o certificado ou recuperar o nome do host. Quando isso é combinado com um aplicativo como o Skype for Business que não envia um campo Server Name Indication (SNI) em sua mensagem de saudação do cliente TLS, torna-se necessário ignorar totalmente esse tráfego. O AsyncOS 11.8 introduziu a capacidade de ignorar o tráfego com base apenas no endereço IP de destino, sem verificações de certificado para lidar com esse cenário.

Monitores e alertas

Monitores CLI

A CLI SWA fornece comandos para monitoramento em tempo real de processos importantes. Os mais úteis são os comandos que mostram estatísticas relacionadas ao processo prox. O comando status detail é uma boa fonte para um resumo do uso de recursos e métricas de desempenho, incluindo tempo de atividade, largura de banda usada, latência de resposta, número de conexões e muito mais. Veja um exemplo de saída desse 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
```

O comando rate mostra informações em tempo real sobre a porcentagem de CPU usada pelo processo prox, bem como o número de Solicitações por Segundo (RPS) e estatísticas de cache. Esse comando continua a sondar e exibir novas saídas até que sejam interrompidos. Este é um exemplo de saída deste 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
```

O comando tcpservices exibe informações sobre as portas de escuta de processos selecionadas. Uma explicação de cada processo e a combinação de endereço e porta também é exibida:

```
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
```

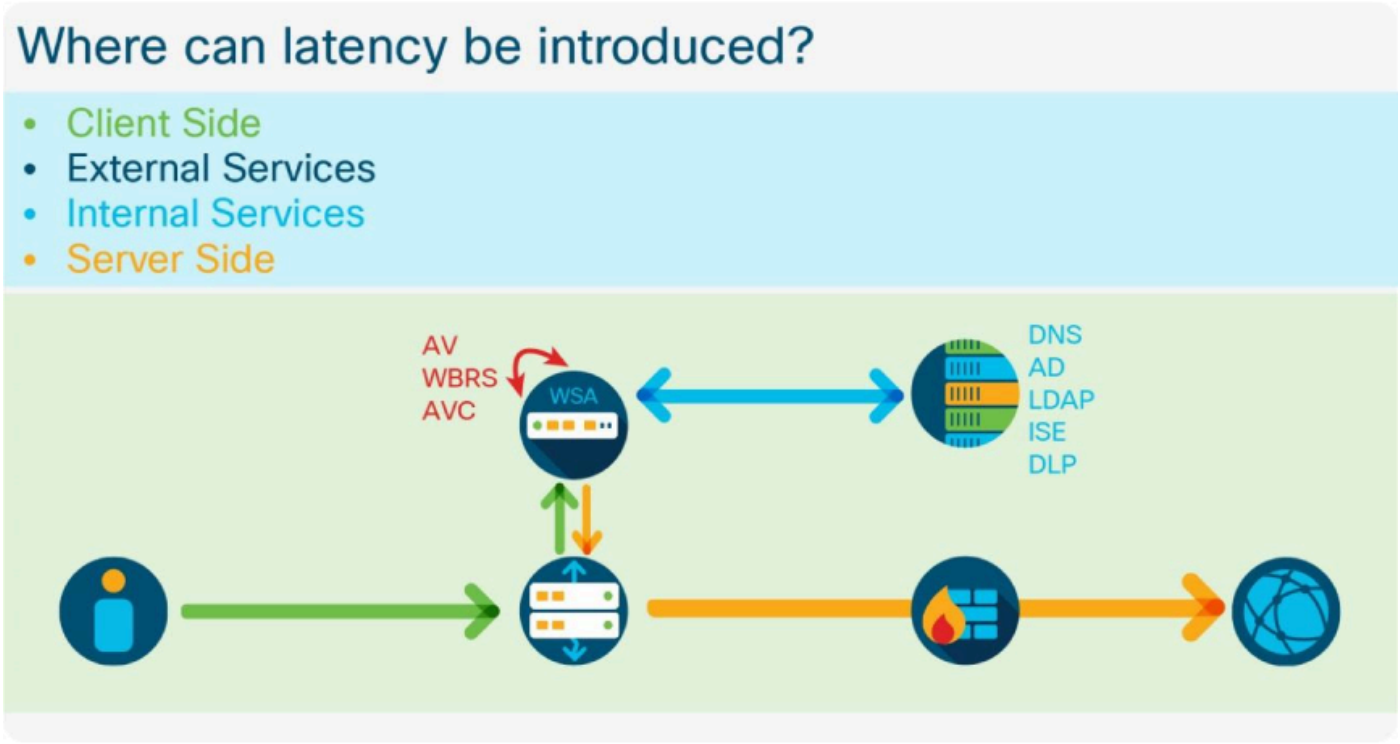
```
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         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
```

Registro

O tráfego da Web é altamente dinâmico e variado. Após a conclusão de uma implantação de

proxy, é importante reavaliar regularmente a quantidade e a composição do tráfego que está sendo passado pelo dispositivo. Você deve verificar a porcentagem de tráfego descriptografado regularmente (uma vez por trimestre) para garantir que o tamanho seja consistente com as expectativas e especificações da instalação inicial. Isso pode ser feito com um produto de gerenciamento de logs, como o Advanced Web Security Reporting (AWSR), ou com comandos simples do Bash ou do PowerShell com os logs de acesso. O número de RPS também deve ser reavaliado regularmente para garantir que o dispositivo tenha sobrecarga suficiente para lidar com picos de tráfego e possível failover em uma configuração de alta disponibilidade com balanceamento de carga.

O registro track_stats é anexado a cada cinco minutos e inclui várias seções de saída diretamente relacionadas ao processo prox e seus objetos na memória. Mais úteis no monitoramento de desempenho são as seções que mostram a latência média de vários processos de solicitação, incluindo tempo de pesquisa de DNS, tempo de verificação do mecanismo AV e muitos outros campos úteis. Esse registro não é configurável na GUI ou na CLI e só pode ser acessado por meio do protocolo SCP (Secure Copy Protocol) ou do FTP (File Transfer Protocol). Esse é o registro mais importante a ser obtido durante a solução de problemas de desempenho, portanto, ele deve ser interrogado com frequência.



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 waiting for a response.
- May indicate an upstream issues-keep investigating!
- Access logs can show this in custom field **% : 1>**

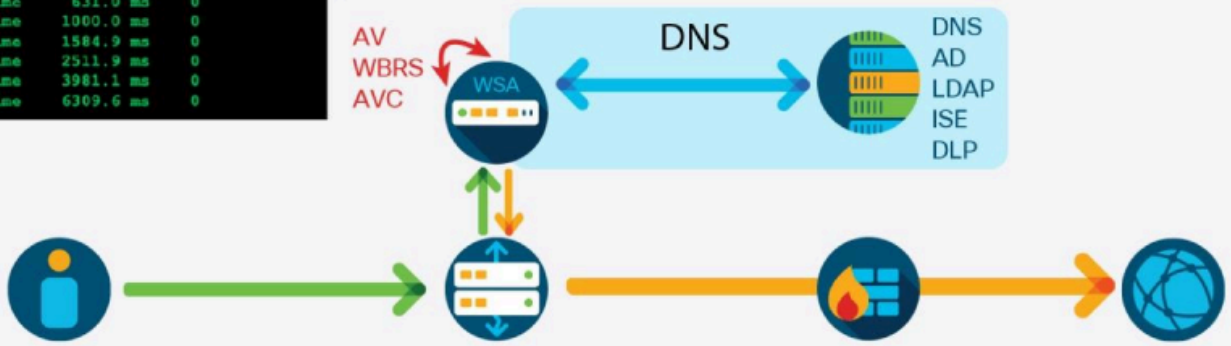
%:1>	x-p2c-first-byte-time	Wait-time for first byte written to client

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 for a DNS response.
- Calls for investigation for your DNS resolvers (or path to them).
- **access logs** can show this in custom field **% : >d**

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

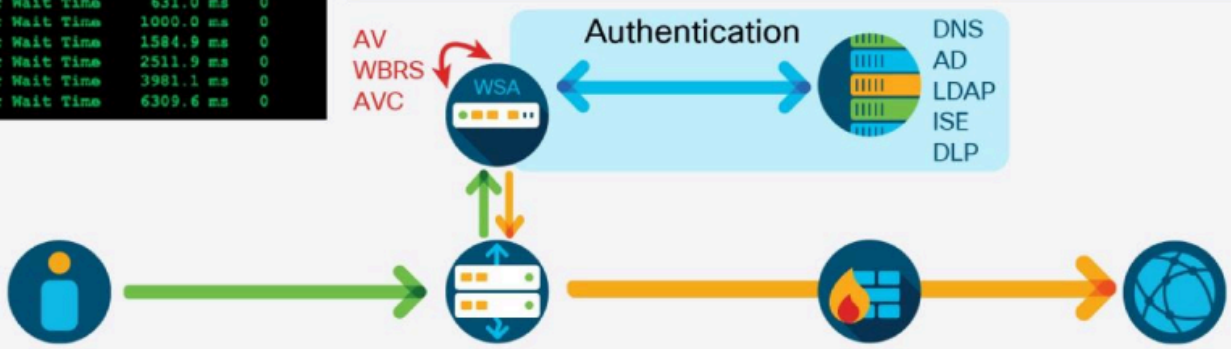


Authentication latency

```
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 **"Auth Helper Service Wait Time."**
- Use the first to get pure auth time without the request time added.
- **access logs** can show this in custom field **% : >a**

%:<a	x-p2p-auth-wait-time	Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.

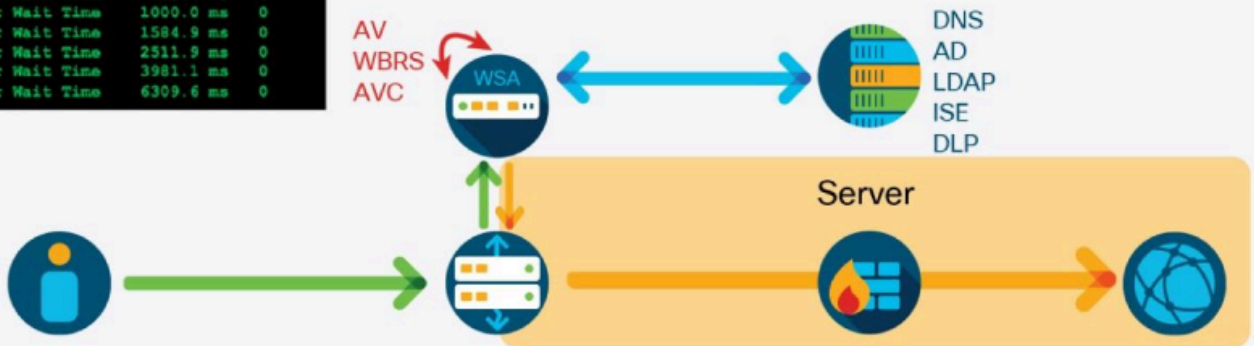


Server latency-wait time

```
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 for the first byte of the server response.
- Calls for investigation of your upstream devices and WAN connection.
- **access logs** can show this in custom field **% : >1**

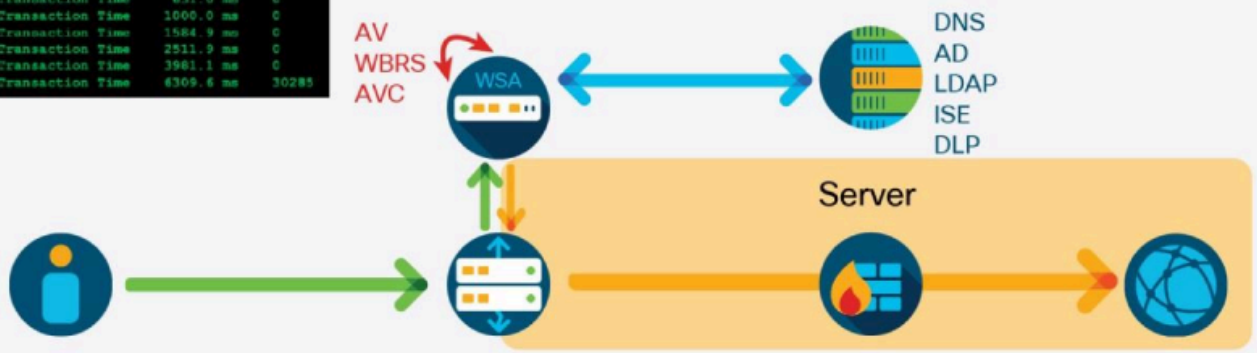
%:>1	x-s2p-first-byte-time	Wait-time for first response byte from server



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-side transaction to complete.
- Calls for investigation of your upstream devices and WAN connection.
- No **access logs** custom field, but can be determined by a combinationof them.



Internal services latency-not exhaustive

Sophos Response Body Service Time	10.0 ms	0
Sophos Response Body Service Time	17.3 ms	0
Sophos Response Body Service Time	30.0 ms	0
Sophos Response Body Service Time	52.1 ms	0
Sophos Response Body Service Time	90.3 ms	0
Sophos Response Body Service Time	156.5 ms	0

Adaptive Scanning Service Time	1.0 ms	2
Adaptive Scanning Service Time	1.6 ms	0
Adaptive Scanning Service Time	2.5 ms	0
Adaptive Scanning Service Time	4.0 ms	0
Adaptive Scanning Service Time	6.3 ms	0
Adaptive Scanning Service Time	10.0 ms	0

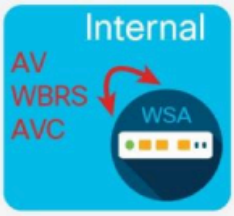
McAfee Response Body Service Time	10.0 ms	0
McAfee Response Body Service Time	17.3 ms	0
McAfee Response Body Service Time	30.0 ms	0
McAfee Response Body Service Time	52.1 ms	0
McAfee Response Body Service Time	90.3 ms	0
McAfee Response Body Service Time	156.5 ms	0

AVC Header Scan Service Time	10.0 ms	8398
AVC Header Scan Service Time	17.3 ms	11
AVC Header Scan Service Time	30.0 ms	3
AVC Header Scan Service Time	52.1 ms	0
AVC Header Scan Service Time	90.3 ms	0
AVC Header Scan Service Time	156.5 ms	0

Webroot Response Body Service Time	10.0 ms	0
Webroot Response Body Service Time	14.6 ms	0
Webroot Response Body Service Time	21.4 ms	0
Webroot Response Body Service Time	31.3 ms	0
Webroot Response Body Service Time	45.7 ms	0
Webroot Response Body Service Time	66.9 ms	0

Ironport Data Security Service Time	10.0 ms	0
Ironport Data Security Service Time	17.3 ms	0
Ironport Data Security Service Time	30.0 ms	0
Ironport Data Security Service Time	52.1 ms	0
Ironport Data Security Service Time	90.3 ms	0
Ironport Data Security Service Time	156.5 ms	0

WBRS Service Time	1.0 ms	3917
WBRS Service Time	1.6 ms	198
WBRS Service Time	2.5 ms	60
WBRS Service Time	4.0 ms	16
WBRS Service Time	6.3 ms	6
WBRS Service Time	10.0 ms	6



See the user guide for all custom fields associated with these values.

Uma linha de log SHD individual é gravada a cada 60 segundos e contém muitos campos importantes para o monitoramento de desempenho, incluindo latência, RPS e conexões totais do lado do cliente e do lado do servidor. Este é um exemplo de uma linha de 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 61
Fri Nov 11 14:17:42 2022 Info: Status: CPULd 2.6 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 10532 Latency 77
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 79
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 140
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
```

Campos personalizados adicionais podem ser adicionados aos access_logs que denotam informações de latência para solicitações individuais. Esses campos incluem a resposta do servidor, a resolução DNS e a latência do scanner AV. Os campos devem ser adicionados ao registro para obter informações valiosas a serem usadas na solução de problemas. Esta é a sequência de caracteres de campo personalizado recomendada para uso:

```
[ 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<,
```

```
a; DNS response = %:
```

```
d, WBRS response = %:
```

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

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

As informações de desempenho derivadas desses valores são as seguintes:

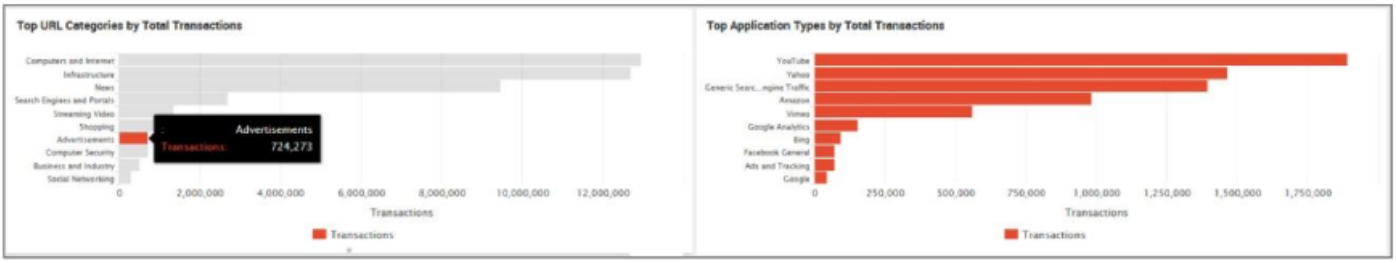
Campo personalizado	Descrição
%:<a	Tempo de espera para receber a resposta do processo de autenticação do proxy da Web, depois que o Proxy da Web enviou a solicitação.
%:<b	Tempo de espera para gravar corpo de solicitação no servidor após cabeçalho.
%:<d	Tempo de espera para receber a resposta do processo DNS do proxy da Web, depois que o Proxy da Web enviou a solicitação.
%:<h	Tempo de espera para gravar o cabeçalho da solicitação no servidor após o primeiro byte.
%:<r	Tempo de espera para receber a resposta dos filtros de reputação da Web, depois que o proxy da Web enviou a solicitação.
%:<s	Tempo de espera para receber o veredito do processo antispyware do proxy da Web, depois que o proxy da Web enviou a solicitação.
%:>	Tempo de espera para o primeiro byte de resposta do servidor.
%:>a	O tempo de espera para receber a resposta do processo de autenticação do proxy da Web inclui o tempo necessário para que o proxy da Web envie a solicitação.
%:>b	Tempo de espera para o corpo de resposta completo após o recebimento do cabeçalho.
%:>c	Tempo necessário para que o proxy da Web leia uma resposta do cache de disco.
%:>d	O tempo de espera para receber a resposta do processo DNS do proxy da Web inclui o tempo necessário para que o proxy da Web envie a solicitação.
%:>h	Tempo de espera para o cabeçalho do servidor após o primeiro byte de resposta.
%:>r	O tempo de espera para receber o veredito dos filtros de reputação da Web inclui o tempo necessário para que o proxy da Web envie a solicitação.
%:>s	O tempo de espera para receber o veredito do processo antispyware do proxy da Web inclui o tempo necessário para que o proxy da Web envie a solicitação.
%:1<	Tempo de espera para o primeiro byte de solicitação da nova conexão do cliente.
%:1>	Tempo de espera para o primeiro byte gravado no cliente.
%:b<	Tempo de espera para concluir o corpo do cliente.
%:b>	Tempo de espera para a gravação completa do corpo no cliente.

%:e>	Aguarde para receber a resposta do mecanismo de varredura da AMP, depois que o proxy da Web enviou a solicitação.
%:e<	O tempo de espera para receber o veredito do mecanismo de varredura da AMP inclui o tempo necessário para que o proxy da Web envie a solicitação.
%:h<	Tempo de espera para cabeçalho completo do cliente após o primeiro byte.
%:h>	Tempo de espera para a conclusão do cabeçalho gravado no cliente.
%:m<	O tempo de espera para receber o veredito do mecanismo de varredura da McAfee inclui o tempo necessário para que o proxy da Web envie a solicitação.
%:m>	Aguarde para receber a resposta do mecanismo de varredura da McAfee, depois que o proxy da Web enviou a solicitação.
% F	Porta de origem do cliente.
% p	Porta do servidor Web.
% k	Endereço IP da origem de dados (Endereço IP do Servidor Web).
%:w<	O tempo de espera para receber o veredito do mecanismo de varredura do Webroot inclui o tempo necessário para que o proxy da Web envie a solicitação.
%:w>	Tempo de espera para receber a resposta do mecanismo de varredura Webroot, depois que o proxy da Web enviou a solicitação.

O modelo de licenciamento SWA permite a reutilização de licenças de dispositivos físicos para dispositivos virtuais. Você pode aproveitar isso e implantar dispositivos SWAv de teste para uso em ambiente de laboratório. Novos recursos e configurações podem ser testados dessa forma para garantir estabilidade e confiabilidade sem e ao mesmo tempo sem violar os termos de licenciamento.

Relatório de Segurança da Web Avançado (AWSR)

O AWSR deve ser aproveitado para aproveitar ao máximo os dados de relatório do SWA. Especialmente em ambientes onde muitos SWAs são implantados, essa solução é muitas vezes mais escalável do que a utilização de relatórios centralizados em um Security Management Appliance (SMA), bem como fornece atributos de relatórios personalizados que adicionam uma imensa profundidade e personalização aos dados. Os relatórios podem ser agrupados e personalizados para atender às necessidades de qualquer empresa. O grupo Cisco Advanced Services deve ser aproveitado no dimensionamento do AWSR.



Alerta por e-mail

O sistema de alerta por e-mail integrado no SWA é melhor aproveitado como um sistema de

alerta de linha de base. Ele deve ser ajustado adequadamente para atender às necessidades do administrador, pois pode ser muito ruidoso se todos os eventos informativos estiverem ativados. É mais importante limitar os alertas e monitorá-los ativamente do que alertá-los sobre tudo e ignorá-los como spam.

Configurações de alerta	Configuração
Endereço De a ser usado ao enviar alertas	Gerado automaticamente
Número inicial de segundos a aguardar antes de enviar um alerta duplicado	300 Segundos
Número máximo de segundos a aguardar antes de enviar um alerta duplicado	3600 Segundos

Monitoramento de disponibilidade

Há dois métodos que podem ser empregados para monitorar a disponibilidade de um proxy da Web.

1. O primeiro é o monitoramento de Camada 3 (L3), que testa se o endereço IP do dispositivo está acessível na rede. A maneira mais simples de testar isso é enviar uma solicitação de ICMP Echo (ping) ao endereço em intervalos regulares e verificar se há um pacote Reply. Os atributos da resposta, como TTL e latência, podem ser analisados para determinar a integridade da camada de rede.
2. É possível que um dispositivo possa responder aos pings, mas que os processos de proxy não respondam ou sejam intermitentes. Por causa disso, é aconselhável empregar um monitor da camada 7 (L7), que envia uma solicitação de proxy explícita para o dispositivo e espera um código de resposta HTTP 200 OK. Isso testa não apenas a acessibilidade da interface de rede, mas também a capacidade de resposta dos serviços de proxy e a viabilidade dos serviços upstream se um recurso externo for solicitado. Esse tipo de monitoramento geralmente assume a forma de uma solicitação HTTP HEAD explícita que solicita que o proxy se conecte a um recurso. O método HEAD solicita os cabeçalhos que serão retornados e o cliente deve enviar uma solicitação GET, mas inclui apenas os cabeçalhos de resposta e nenhum dado.
    - Se você usar uma ferramenta de monitoramento L7 ou um script, é importante garantir que o tráfego seja isento de autenticação. Caso contrário, isso resultará em falhas de autenticação regulares e no consumo de recursos. Quando você usa uma sequência de caracteres de agente de usuário personalizada na ferramenta de monitoramento, deve ser empregado para identificar o tráfego. Mesmo que o tráfego esteja isento de autenticação, ele ainda pode ser restrito do acesso desnecessário à Internet através das políticas de acesso.

Quando você usa um ou mais desses métodos, um administrador deve estabelecer uma linha de base de métricas aceitáveis em torno da resposta do proxy e usá-la para criar limites de alerta. Você deve dedicar tempo para reunir as respostas dessas verificações e antes de decidir como configurar os limites e o alerta.

Monitoramento de SNMP

O Simple Network Management Protocol (SNMP) é o principal método para monitorar a integridade do dispositivo. Ele pode ser usado para receber alertas do dispositivo (traps) ou para pesquisar vários Identificadores de objeto (OIDs) para coletar informações. Há muitos OIDs disponíveis no SWA que cobrem tudo, desde o hardware até o uso de recursos, informações de processos individuais e estatísticas de solicitações.

Há uma série de Base de Informações da Máquina (MIB - Machine Information Base) que devem ser monitoradas por motivos relacionados ao hardware e ao desempenho. A lista completa de MIBs pode ser encontrada aqui: https://www.cisco.com/web/ironport/tools/web/asyncosweb-mib.txt.

Esta é uma lista das MIBs recomendadas para monitorar e não uma lista exaustiva:

OID de Hardware	Nome
1.3.6.1.4.1.15497.1.1.1.18.1.3	ID de raid
1.3.6.1.4.1.15497.1.1.1.18.1.2	status de raid
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	fanTable
1.3.6.1.4.1.15497.1.1.1.9.1.2	graus Celsius

Os OIDs são mapeados diretamente para a saída do comando CLI status detail:

OID	Nome	Campo de detalhe de status
Recursos do sistema		
1.3.6.1.4.1.15497.1.1.1.2.0	perCentCPUtilização	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	utilização de memória perCent	RAM
Transações por segundo		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruputNow	Média de transações por segundo no último minuto.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThruput1hrPeak	Máximo de transações por segundo na última hora.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThruput1hrMédia	Média de transações por segundo na última hora.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	Máximo de transações por segundo desde a reinicialização do proxy.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruputLifeMean	Média de transações por segundo desde a reinicialização do proxy.

Largura de banda		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	larguraLarguraCacheTotalAgora	Largura de banda média no último minuto.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	Largura de banda máxima na última hora.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMédia	Largura de banda média na última hora.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	Largura de banda máxima desde a reinicialização do proxy.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	Largura de banda média desde a reinicialização do proxy.
Tempo de resposta		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	acertos de cacheAgora	Taxa média de acertos do cache no último minuto.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	Taxa máxima de acertos do cache na última hora.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMédia	Taxa média de acertos do cache na última hora.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	Taxa máxima de acertos no cache desde a reinicialização do proxy.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	CacheHitsLifeMean	Taxa média de acertos no cache desde a reinicialização do proxy.
Taxa de acertos do cache		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	acertos de cacheAgora	Taxa média de acertos do cache no último minuto.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	Taxa máxima de acertos do cache na última hora.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMédia	Taxa média de acertos do cache na última hora.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	Taxa máxima de acertos no cache desde a reinicialização do proxy.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	CacheHitsLifeMean	Taxa média de acertos no cache desde a reinicialização do proxy.
Conexões		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	Conexões de cliente ociosas.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServidorIdleConns	Conexões de servidor ociosas.
1.3.6.1.4.1.15497.1.2.3.2.8.0	TotalConnsClienteCache	Total de conexões de cliente.
1.3.6.1.4.1.15497.1.2.3.3.8.0	TotalConnsServidorCache	Total de conexões do servidor.

Conclusão

Este guia procura descrever os aspectos mais importantes da configuração, implantação e monitoramento do SWA. Como guia de referência, seu objetivo é fornecer informações valiosas para aqueles que desejam garantir o uso mais eficaz do SWA. As melhores práticas descritas aqui são importantes para a estabilidade, escalabilidade e eficácia do dispositivo como uma ferramenta de segurança. Ele também procura permanecer como um recurso relevante que avança e, portanto, deve ser atualizado com frequência para refletir as alterações nos ambientes de rede e nos conjuntos de recursos do produto.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.