Domande frequenti su Cisco VPN 3000 Concentrator

Sommario

Introduzione

Questo documento risponde alle domande frequenti (FAQ) su Cisco VPN serie 3000 Concentrator.

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Generale

D. Cosa significa il messaggio di errore "Lost Service"?

R. Se non viene inviato traffico tra il concentratore VPN e il client VPN per un periodo di tempo, un pacchetto DPD (Dead Peer Detection) viene inviato dal concentratore VPN al client VPN per verificare che il peer sia ancora presente. In caso di problemi di connettività tra i due peer in cui il client VPN non risponde al concentratore VPN, questo continua a inviare pacchetti DPD per un determinato periodo di tempo. In questo modo il tunnel viene terminato e viene generato l'errore se non riceve una risposta entro il tempo specificato. Fare riferimento all'ID bug Cisco CSCdz45586 (contratto di supporto richiesto).

L'errore dovrebbe essere simile al seguente:

```
SEV=4 AUTH/28 RPT=381 XXX.XXX.XXX.XX User [SomeUser] disconnected:
Duration: HH:MM:SS Bytes xmt: 19560 Bytes rcv: 17704 Reason:
Lost Service YYYY/MM/DD HH:MM:SS XXX.XXX.XXX.XXX
syslog notice
45549 MM/DD/YYYY HH:MM:SS SEV=4 IKE/123 RPT=XXX.XXX.XXX.XXX
Group [SomeDefault] User [SomeUser]
IKE lost contact with remote peer, deleting connection (keepalive type: DPD)
```

Causa: Il peer IKE remoto non ha risposto a keepalive entro la finestra di tempo prevista, quindi la connessione al peer IKE è stata eliminata. Il messaggio include il meccanismo keep-alive utilizzato. Questo problema è riproducibile solo se l'interfaccia pubblica viene disconnessa durante una sessione del tunnel attiva. Il cliente deve monitorare la connettività di rete poiché questi eventi vengono generati per individuare la root cause dei potenziali problemi di connettività di rete.

Disabilitare IKE keepalive accedendo a **%System Root%\Programmi\Cisco Systems\VPN**

Client\Profiles sul PC client in cui si è verificato il problema e modificare il **file PCF** (se applicabile) per la connessione.

Modificare 'ForceKeepAlives=0' (impostazione predefinita) in '**ForceKeepAlives=1**'.

Se il problema persiste, aprire una richiesta di servizio con il supporto tecnico Cisco e specificare il "Visualizzatore dei log" del client e VPN Concentrator eseguirà la registrazione quando il problema si verifica.

D. Qual è il significato del messaggio di errore "`q_send`" failures detected for EMQ1 queue?

R. Questo messaggio di errore viene visualizzato quando il buffer contiene troppi eventi/informazioni di debug. Non ha alcun impatto negativo se non la possibilità di perdere alcuni messaggi relativi agli eventi. Provare a ridurre gli eventi al numero minimo necessario per impedire la visualizzazione del messaggio.

D. Il gruppo eliminato è ancora visualizzato nella configurazione di VPN Concentrator. Come si elimina questo?

R. Copiare la configurazione in un editor di testo (ad esempio Blocco note) e modificare o eliminare manualmente le informazioni sul gruppo interessato indicate da **[ipaddrgrouppool #.0]**. Salvare la configurazione e caricarla su VPN Concentrator. Di seguito è riportato un esempio.

```
!--- Change to 14.1 or any other number that is not in use !--- any number other than 0).
[ipaddrgrouppool 14.0] rowstatus=1 rangename= startaddr=172.18.124.1 endaddr=172.18.124.2
```

D. È possibile avere più server SDI primari?

R. I concentratori VPN 3000 sono in grado di scaricare solo un file segreto nodo alla volta. In SDI versione precedente alla 5.0, è possibile aggiungere più server SDI, ma tutti devono condividere lo stesso file segreto del nodo (considerarlo come server principale e di backup). In SDI versione 5.0, è possibile immettere solo un server SDI primario (i server di backup sono elencati nel file segreto del nodo) e i server di replica.

D. Viene visualizzato il messaggio di errore "`Certificato SSL scadrà tra 28 giorni`". Cosa devo fare?

R. Il messaggio indica che il certificato SSL (Secure Sockets Layer) scadrà tra 28 giorni. Questo certificato viene utilizzato per esplorare la gestione Web tramite HTTPS. È possibile lasciare il certificato con le impostazioni predefinite oppure configurare opzioni diverse prima di generare il nuovo certificato. Selezionare **Configurazione > Sistema > Protocolli di gestione > SSL** per eseguire questa operazione. Selezionare **Amministrazione > Gestione certificati** e fare clic su **Genera** per rinnovare il certificato.

Per problemi di sicurezza sul concentratore VPN e per impedire accessi non autorizzati, disabilitare HTTP e/o HTTPS sull'interfaccia pubblica da **Configurazione > Gestione policy > Gestione traffico > Filtri**. Se è necessario accedere al proprio concentratore VPN tramite Internet tramite HTTP o HTTPS, è possibile specificare l'accesso in base all'indirizzo di origine scegliendo **Amministrazione > Diritti di accesso > Lista di controllo di accesso**. Per ulteriori informazioni,

utilizzare il menu? nell'angolo superiore destro della finestra.

D. Come è possibile visualizzare le informazioni utente nel database interno degli utenti? Non è visibile quando si controlla il file config.

A. Selezionare **Amministrazione > Diritti di accesso > Impostazioni di accesso**, scegliere **Config File Encryption=None**, quindi salvare la configurazione per visualizzare utenti e password. Dovrebbe essere possibile cercare l'utente specifico.

D. Quanti utenti possono memorizzare il database interno?

R. Il numero di utenti dipende dalla versione e viene specificato nella sezione **Configurazione > Gestione utente** della Guida dell'utente per la release VPN 3000 Concentrator. In VPN 3000 release da 2.2 a 2.5.2 è possibile un totale di 100 utenti o gruppi (la somma di utenti e gruppi deve essere uguale o inferiore a 100). In VPN 3000 release 3.0 e successive, il numero per i concentratori 3005 e 3015 rimane 100. Per i concentratori VPN 3030 e 3020, il numero è 500, per i concentratori VPN 3060 o 3080 rators, il numero è 1000. Inoltre, l'utilizzo di un server di autenticazione esterno migliora la scalabilità e la gestibilità.

D. Qual è la differenza tra il gateway predefinito del tunnel e il gateway predefinito?

R. VPN 3000 Concentrator usa il gateway predefinito del tunnel per indirizzare gli utenti tunneling all'interno della rete privata (di solito il router interno). VPN Concentrator utilizza il gateway predefinito per indirizzare i pacchetti a Internet (in genere al router esterno).

D. Se il concentratore VPN 3000 viene posizionato dietro un firewall o un router che esegue elenchi di controllo di accesso, quali porte e protocolli è necessario consentire?

R. In questo grafico vengono elencate le porte e i protocolli.

Servizio	Numero protocollo	Porta di origine	Porta di destinazione
Connessione controllo PPTP	6 (TCP)	1023	1723
PPTP Tunnel Encapsulation	47 (GRE)	N/D	N/D
Gestione delle chiavi ISAKMP/IPSec	17 (UDP)	500	500
IPSec Tunnel Encapsulation	50 (ESP)	N/D	N/D
Trasparenza NAT IPSec	17 (UDP)	10000 (impostazione predefinita)	10000 (impostazione predefinita)

Nota: la porta trasparente NAT (Network Address Translation) è configurabile su qualsiasi valore

compreso nell'intervallo da 4001 a 49151. Nelle versioni 3.5 o successive, è possibile configurare IPsec su TCP passando a **Configurazione > Sistema > Protocolli di tunneling > IPSec > IPSec su TCP**. È possibile immettere fino a 10 porte TCP separate da virgole (1 - 65535). Se questa opzione è configurata, verificare che queste porte siano consentite nel firewall o nel router che esegue gli elenchi di controllo di accesso.

D. Come posso ripristinare VPN Concentrator ai valori predefiniti?

R. Dalla schermata File Management, eliminare il file "config" e riavviare. Se il file viene eliminato accidentalmente, viene conservata una copia di backup, "config.bak".

D. È possibile utilizzare TACACS+ per l'autenticazione amministrativa? Cosa devo tenere in mente mentre lo faccio?

R. Sì, a partire da VPN 3000 Concentrator release 3.0, è possibile usare TACACS+ per l'autenticazione amministrativa. Dopo aver configurato TACACS+, verificare l'autenticazione prima di disconnettersi. Una configurazione errata di TACACS+ può bloccarvi. Per disabilitare TACACS+ e risolvere il problema, è necessario effettuare l'accesso alla porta console.

D. Cosa fare quando la password amministrativa viene dimenticata?

R. Nelle versioni 2.5.1 e successive, collegare un PC alla porta console di VPN Concentrator utilizzando un cavo seriale RS-232 straight-through con il PC impostato su:

- 9600 bit al secondo
- 8 bit di dati
- nessuna parità
- 1 bit di stop
- controllo del flusso hardware attivato
- VT100 emulation

Riavviare VPN Concentrator. Al termine del controllo diagnostico, sulla console viene visualizzata una riga di tre punti (...). Premere **CTRL-C** entro tre secondi dalla visualizzazione dei punti. Viene visualizzato un menu che consente di ripristinare le password di sistema ai valori predefiniti.

D. Qual è lo scopo del nome e della password del gruppo?

R. Il nome e la password del gruppo vengono utilizzati per creare un hash che viene quindi utilizzato per creare un'associazione di protezione.

D. VPN Concentrator proxy ARP per conto degli utenti del tunneling?

R. Sì.

D. Dove posizionare VPN 3000 Concentrator in relazione al firewall di rete?

R. Il VPN 3000 Concentrator può essere posizionato davanti, dietro, parallelamente o nella zona demilitarizzata (DMZ) di un firewall. Non è consigliabile avere le interfacce pubblica e privata nella stessa LAN virtuale (VLAN).

D. È possibile disabilitare il proxy ARP sul Cisco VPN 3000 Concentrator?

R. Impossibile disabilitare Proxy Address Resolution Protocol (ARP) su Cisco VPN 3000 Concentrator.

D. Dove posso trovare i bug riscontrati su VPN 3000 Concentrator?

R. Per informazioni dettagliate sui bug, è possibile usare Bug Search Tool (contratto di assistenza richiesto).

D. Dove posso trovare gli esempi di configurazione per VPN 3000 Concentrator?

R. Oltre alla documentazione di VPN 3000 Concentrator, ulteriori esempi di configurazione sono disponibili nella pagina di supporto di Cisco VPN 3000 Concentrator.

D. Come è possibile aumentare la registrazione per ottenere debug migliori per eventi specifici?

R. È possibile passare a **Configurazione > Sistema > Eventi > Classi** e configurare gli eventi specifici (ad esempio IPsec o PPTP) per ottenere debug migliori. Il debug deve essere attivato solo per la durata dell'esercizio di risoluzione dei problemi, in quanto può causare una riduzione delle prestazioni. Per il debug IPsec, attivare IKE, IKEDBG, IPSEC, IPSECDBG, AUTH e AUTHDBG. Se si utilizzano certificati, aggiungere la classe CERT all'elenco.

D. Come posso monitorare il traffico verso VPN 3000 Concentrator?

R. L'interfaccia HTML fornita con VPN 3000 Concentrator consente di disporre di funzionalità di monitoraggio di base se si utilizza **Monitoraggio > Sessioni**. VPN 3000 Concentrator può anche essere monitorato tramite il protocollo SNMP (Simple Network Management Protocol) utilizzando un programma di gestione SNMP a scelta. In alternativa, è possibile acquistare Cisco VPN / Security Management Solution (VMS). Cisco VMS fornisce funzionalità chiave per assistere l'utente nell'implementazione della serie VPN 3000 Concentrator e richiedere il monitoraggio approfondito dell'accesso remoto e delle VPN da sito a sito basate su IPsec, L2TP e PPTP. Fare riferimento a VPN Security Management Solution per ulteriori dettagli su VMS.

D. Cisco VPN serie 3000 Concentrator dispone di un firewall integrato? In caso affermativo, quali funzionalità sono supportate?

R. Anche se la serie dispone di funzionalità di filtro/porta stateless e di NAT, Cisco consiglia di utilizzare un dispositivo come Cisco Secure PIX Firewall per il firewall aziendale.

D. Quali opzioni di routing e protocolli VPN sono supportati da Cisco VPN 3000 Concentrator Series?

R. La serie supporta le seguenti opzioni di instradamento:

- Protocollo RIP (Routing Information Protocol)
- RIP2
- OSPF (Open Shortest Path First)

- route statiche
- Protocollo VRRP (Virtual Router Redundancy Protocol)

I protocolli VPN supportati includono PPTP (Point-to-Point Tunneling Protocol), L2TP, L2TP / IPsec e IPsec con o senza dispositivo NAT tra VPN 3000 e il client finale. IPsec tramite NAT è noto come trasparenza NAT.

D. Quali sistemi/meccanismi di autenticazione supporta Cisco VPN 3000 Concentrator Series per PC client?

R. Sono supportati i proxy NT Domain, RADIUS o RADIUS, RSA Security SecurID (SDI), i certificati digitali e l'autenticazione interna.

D. È possibile eseguire NAT (Network Address Translation) statico per gli utenti che utilizzano VPN 3000 Concentrator?

R. È possibile eseguire solo Port Address Translation (PAT) per gli utenti che escono. Non è possibile eseguire operazioni NAT statiche sul concentratore VPN 3000.

D. Come è possibile assegnare un indirizzo IP statico a uno specifico utente PPTP (Point-to-Point Tunneling Protocol) o IPsec tramite il concentratore VPN 3000?

R. Nell'elenco viene spiegato come assegnare gli indirizzi IP statici:

- **Utenti PPTP**Nella sezione Gestione indirizzi IP, oltre a scegliere le opzioni del pool o del protocollo DHCP (Dynamic Host Configuration Protocol), selezionare l'opzione **Usa indirizzo client**. Quindi, definire l'utente e l'indirizzo IP in VPN 3000 Concentrator. Questo utente ottiene sempre l'indirizzo IP configurato nel concentratore VPN durante la connessione.
- **Utenti IPSec**Nella sezione Gestione indirizzi IP, oltre a scegliere le opzioni del pool o DHCP, selezionare l'opzione **Usa indirizzo del server di autenticazione**. Quindi, definire l'utente e l'indirizzo IP in VPN 3000 Concentrator. Questo utente ottiene sempre l'indirizzo IP configurato nel concentratore VPN durante la connessione. Tutti gli altri che appartengono allo stesso gruppo o ad altri gruppi ricevono un indirizzo IP dal pool globale o da DHCP.Con il software Cisco VPN 3000 Concentrator versione 3.0 e successive, è possibile configurare un pool di indirizzi su base di gruppo. Questa funzione consente di assegnare un indirizzo IP statico anche a un utente specifico. Se si configura un pool per un gruppo, l'utente con indirizzo IP statico ottiene l'indirizzo IP assegnato e gli altri membri dello stesso gruppo ottengono gli indirizzi IP dal pool di gruppi. Ciò è valido solo quando si utilizza VPN Concentrator come server di autenticazione.

Nota: se si utilizza un server di autenticazione esterno, è necessario utilizzare tale server per assegnare gli indirizzi correttamente.

D. Quali sono alcuni problemi noti di compatibilità con i prodotti PPTP di Microsoft e VPN 3000 Concentrator?

R. Queste informazioni sono basate sul software VPN 3000 Concentrator versione 3.5 e successive; VPN serie 3000 concentrator, modelli 3005, 3015, 3020, 3030, 3060, 3080; e sistemi operativi Microsoft Windows 95 e versioni successive.

- **Windows 95 DUN (Dial-Up Networking) 1.2**Microsoft Point-to-Point Encryption (MPPE) non è supportato in DUN 1.2. Per connettersi utilizzando MPPE, installare Windows 95 DUN 1.3. È possibile scaricare l'aggiornamento a Microsoft DUN 1.3 dal sito Web Microsoft.
- **Windows NT 4.0**Windows NT è supportato completamente per le connessioni PPTP (Point-to-Point Tunneling Protocol) al concentratore VPN. Service Pack 3 (SP3) o versione successiva. Se è in esecuzione SP3, installare le patch di Prestazioni e protezione PPTP. Per informazioni sull'aggiornamento delle prestazioni e della sicurezza PPTP Microsoft per WinNT 4.0, visitare il sito Web Microsoft .Si noti che il Service Pack 5 a 128 bit non gestisce correttamente le chiavi MPPE e che PPTP potrebbe non riuscire a passare i dati. In questo caso, nel registro eventi viene visualizzato il seguente messaggio:

  ```
  103 12/09/1999 09:08:01.550 SEV=6 PPP/4 RPT=3 80.50.0.4
  User [ testuser ]
  disconnected. Experiencing excessive packet decrypt failure.
  ```

  Per risolvere il problema, scaricare l'aggiornamento per Come ottenere le versioni più recenti di Windows NT Service Pack 6a e Windows NT 4.0 Service Pack 6a Disponibile. Per ulteriori informazioni, vedere l'articolo Microsoft MPPE Keys Not Handled Correct for a 128-Bit MS-CHAP Request .

D. Qual è il numero massimo di filtri consentiti su un concentratore VPN 3000?

R. Il numero massimo di filtri che è possibile aggiungere a un'unità VPN 30xx (anche a 3030 o 3060) è fissato a 100. Per ulteriori informazioni su questo problema, consultare l'ID bug Cisco CSCdw86558 (è necessario il contratto di supporto).

D. Qual è il numero massimo di route nella linea 30xx di VPN concentrator?

R. Il numero massimo di cicli di lavorazione è:

- In precedenza, VPN 3005 Concentrator disponeva di un massimo di 200 route. Questo numero è ora aumentato a 350 rotte. Per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCeb35779 (contratto di supporto richiesto).
- VPN 3030 Concentrator è stato testato fino a 10.000 route.
- Il limite della tabella di routing sui concentratori VPN 3030, 3060 e 3080 è proporzionale alle risorse e alla memoria disponibili in ciascun dispositivo.
- VPN 3015 Concentrator non ha un limite massimo predefinito. Ciò vale per i protocolli RIP (Routing Information Protocol) e OSPF (Open Shortest Path First).
- Il concentratore VPN 3020: a causa di una limitazione di Microsoft, i PC Windows XP non sono in grado di ricevere un numero elevato di route statiche senza classificazione (CSR, Classless Static Routes). Il concentratore VPN 3000 limita il numero di CSR inseriti in una risposta al messaggio INFORM DHCP quando configurato per tale operazione. VPN 3000 Concentrator limita il numero di route a 28-42, a seconda della classe.

D. Come è possibile cancellare completamente le statistiche sull'interfaccia di VPN 3000 Concentrator?

A. Selezionare **Monitoraggio > Statistiche > MIB-II > Ethernet** e reimpostare le statistiche per cancellare le statistiche per la sessione corrente. Ricordatevi che questo non cancella completamente le statistiche. È necessario riavviare per reimpostare effettivamente le statistiche (anziché reimpostarle per il monitoraggio).

D. Quali porte devo consentire a VPN Concentrator per la comunicazione NTP (Network Time Protocol)?

R. Consentire le porte TCP e UDP 123.

D. Quali sono le funzioni delle porte UDP 625xx?

R. Le porte vengono usate per la comunicazione VPN Client tra l'Extender NDIS deterministico/shim (DNE) effettivo e lo stack TCP/IP del PC e sono destinate solo allo sviluppo interno. Ad esempio, la porta 62515 viene utilizzata dal client VPN per inviare informazioni al log del client VPN. Di seguito sono illustrate altre funzioni delle porte.

- 62514 - Cisco Systems, Inc. Servizio VPN per driver IPsec di Cisco Systems
- 62515 - Driver IPsec di Cisco Systems per servizio VPN di Cisco Systems, Inc.
- 62516 - Cisco Systems, Inc. VPN Service to XAUTH
- 62517 - XAUTH to Cisco Systems, Inc. VPN Service
- 62518 - Cisco Systems, Inc. VPN Service to CLI
- 62519 - CLI to Cisco Systems, Inc VPN Service
- 62520 - Cisco Systems, Inc. VPN Service to UI
- 62521 - Interfaccia utente per Cisco Systems, Inc. VPN Service
- 62522 - Messaggi di log
- 62523 - Connection Manager per Cisco Systems, Inc. VPN Service
- 62524 - PPPTool per Cisco Systems, Inc. VPN Service

D. È possibile rimuovere la barra mobile WebVPN?

R. Non è possibile rimuovere la barra degli strumenti mobile né evitare di caricare la barra degli strumenti mobile mentre si stabilisce la sessione WebVPN. Questo perché quando si chiude questa finestra la sessione viene terminata immediatamente e quando si tenta di accedere di nuovo la finestra viene caricata di nuovo. Questo è il modo in cui le sessioni WebVPN sono state progettate originariamente. È possibile chiudere la finestra principale, ma non quella mobile.

Software

D. WebVPN supporta Outlook Web Access (OWA) 2003?

R. Il supporto di OWA 2003 per WebVPN su VPN 3000 Concentrator è ora disponibile con download della versione 4.1.7 (è richiesto il contratto di supporto).

D. Dove posso ottenere le ultime revisioni software per VPN 3000 Concentrator?

R. Tutti i Cisco VPN 3000 concentrator sono forniti con il codice più recente, ma gli utenti possono controllare i download (è richiesto un contratto di supporto) per verificare se è disponibile altro software.

Fare riferimento alla pagina della documentazione di Cisco VPN 3000 Concentrator per la documentazione più recente su VPN 3000 Concentrator.

D. È necessario un server TFTP per aggiornare VPN 3000 Concentrator? Esiste un modo alternativo per aggiornare la confezione?

R. Oltre a utilizzare il protocollo TFTP, è possibile aggiornare VPN Concentrator scaricando il software più recente sul disco rigido. Quindi, da un browser sul sistema in cui si trova il software, andare a **Amministrazione > Aggiornamento software** e trovare il software scaricato sul disco rigido (proprio come aprire un file). Una volta individuato, selezionare la scheda **Upload**.

D. Cosa significa "k9" nei nomi in codice più recenti (ad esempio in "vpn3000-3.0.4.Rel-k9.bin")?

R. La designazione "k9" per il nome immagine ha sostituito la designazione 3DES originariamente utilizzata (ad esempio, vpn3000-2.5.2.F-3des.bin). Pertanto, "k9" indica ora che si tratta di un'immagine 3DES.

D. È consigliabile utilizzare l'opzione di compressione dati del gruppo IPSec per tutti gli utenti?

R. La compressione dei dati aumenta i requisiti di memoria e l'utilizzo della CPU per ogni sessione utente e di conseguenza riduce la velocità di trasmissione complessiva di VPN Concentrator. Per questo motivo, Cisco consiglia di abilitare la compressione dei dati solo se ogni membro del gruppo è un utente remoto che si connette con un modem. Se un membro del gruppo si connette tramite la banda larga, non abilitare la compressione dei dati per il gruppo. Dividere invece il gruppo in due gruppi, uno per gli utenti del modem e l'altro per gli utenti della banda larga. Abilitare la compressione dei dati solo per il gruppo di utenti modem.

Altre caratteristiche avanzate

D. Il bilanciamento del carico funziona con le connessioni da LAN a LAN?

R. Il bilanciamento del carico è effettivo solo sulle sessioni remote avviate con il client software VPN Cisco (versione 3.0 e successive). Tutti gli altri client (PPTP, L2TP) e connessioni LAN-LAN possono connettersi a un concentratore VPN su cui è abilitato il bilanciamento del carico, ma non possono partecipare al bilanciamento del carico.

D. Come decrittografare le password dal file di configurazione?

A. Andare a **Configurazione > Sistema > Protocolli di gestione > XML** e quindi ad **amministrazione | file management selezionare il formato XML**. Utilizzare lo stesso nome o un nome diverso e aprire il file per visualizzare le password.

D. È possibile utilizzare insieme il protocollo VRRP (Virtual Router Redundancy Protocol) e il bilanciamento del carico?

R. Non è possibile utilizzare il bilanciamento del carico con VRRP. In una configurazione VRRP, il dispositivo di backup rimane inattivo a meno che il concentratore VPN attivo non abbia esito negativo. In una configurazione di bilanciamento del carico non sono presenti dispositivi inattivi.

D. Tutto il traffico VPN dei client di accesso remoto deve passare attraverso un tunnel crittografato per raggiungere il concentratore VPN dell'azienda o del provider di servizi? È possibile, ad esempio, che l'accesso semplice ad altri siti venga aperto direttamente tramite la connessione Internet dell'ISP?

R. Sì. Questo concetto è noto come "tunneling suddiviso". Il tunneling ripartito consente un accesso sicuro alle risorse aziendali attraverso un tunnel crittografato, mentre consente l'accesso a Internet direttamente attraverso le risorse dell'ISP (eliminando così la rete aziendale dal percorso per l'accesso al Web). Cisco VPN serie 3000 Concentrator a client VPN Cisco e a client hardware VPN 3002 può supportare lo split tunneling. Per una maggiore sicurezza, questa funzionalità è controllabile dall'amministratore di VPN Concentrator e non dall'utente.

D. È sicuro usare il tunneling ripartito?

R. Il tunneling ripartito consente di navigare in Internet mentre si è connessi tramite il tunnel VPN. Tuttavia, ci pone alcuni rischi se l'utente VPN connesso alla rete aziendale è vulnerabile agli attacchi. In tal caso, è consigliabile utilizzare un firewall personale. Le note di rilascio per una determinata versione di VPN Client descrivono l'interoperabilità con i firewall personali.

D. Come funziona il bilanciamento del carico su Cisco VPN 3000 Concentrator?

R. Il carico viene calcolato come percentuale derivata dalle connessioni attive divisa per il numero massimo di connessioni configurate. Il director tenta sempre di avere il carico minore, in quanto il carico aggiuntivo (intrinseco) è costituito dal mantenimento di tutte le sessioni amministrative da LAN a LAN, dal calcolo del caricamento di tutti gli altri membri del cluster e dal reindirizzamento di tutti i client.

Per un cluster funzionale appena configurato, il director ha un carico di circa l'1% prima di stabilire qualsiasi connessione. Pertanto, il director reindirizza le connessioni al concentratore di backup finché la percentuale di carico sul backup non è superiore alla percentuale di carico sul director. Ad esempio, dati due VPN 3030 concentrator in stati "inattivi", il director ha un carico dell'1%. Al database secondario vengono fornite 30 connessioni (carico del 2%) prima che il director accetti le connessioni.

Per verificare che il director accetti le connessioni, selezionare **Configurazione > Sistema > Generale > Sessioni** e ridurre il numero massimo di connessioni a un numero artificialmente basso per aumentare rapidamente il carico sul concentratore VPN di backup.

D. Quanti dispositivi headend può rilevare il monitor VPN?

R. Il monitor VPN può rilevare 20 dispositivi headend. In uno scenario hub e spoke, le connessioni dai siti remoti vengono monitorate nell'headend. Non è necessario monitorare tutti i siti e gli utenti remoti, in quanto è possibile tracciare tali informazioni sul router dell'hub. Questi headend possono supportare fino a 20.000 utenti remoti o 2.500 siti remoti. Un dispositivo VPN dual-homed che viene inviato ai siti spoke è considerato due dei 20 dispositivi massimi monitorabili.

Informazioni correlate

- Pagina di supporto per Cisco VPN 3000 Concentrator

- Pagina di supporto per i client Cisco VPN 3000
- Documentazione e supporto tecnico – Cisco Systems