

Systemprotokollkonfiguration für die VPN-Router RV016, RV042, RV042G und RV082

Ziel

Ein Systemprotokoll (Syslog) wird verwendet, um Computerdaten zu protokollieren. Sie können die Instanzen definieren, die ein Protokoll generieren. Bei jeder Instanz werden Uhrzeit und Ereignis aufgezeichnet und an einen Syslog-Server oder in einer E-Mail gesendet. Syslog kann dann zur Analyse und Fehlerbehebung in einem Netzwerk bei gleichzeitiger Erhöhung der Netzwerksicherheit eingesetzt werden.

In diesem Dokument wird das Verfahren zur Konfiguration eines Syslog-Servers auf den VPN-Routern RV016, RV042, RV042G und RV082 erläutert.

Unterstützte Geräte

RV016
RV042
RV042G
RV082

Software-Version

v4.2.1.02

Konfiguration von Syslog und Warnmeldungen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Log > System Log (Protokoll > Systemprotokoll)**. Die Seite *Systemprotokoll* wird geöffnet:

System Log

Syslog

Enable Syslog

Syslog Server : (Name or IPv4 / IPv6 Address)

Email

Enable Email Alert

Mail Server : (Name or IPv4 / IPv6 Address)

Send Email to : (Email Address)

Log Queue Length : Entries

Log Time Threshold : Minutes

Log Setting

Alert Log

Syn Flooding IP Spoofing Win Nuke

Ping Of Death Unauthorized Login Attempt

General Log

System Error Messages Deny Policies Allow Policies

Configuration Changes Authorized Login

Syslog

In diesem Abschnitt wird erläutert, wie der Router bei der Ereignisprotokollierung detaillierte Protokolldateien an den Syslog-Server senden kann.

System Log

Syslog

Enable Syslog

Syslog Server : (Name or IPv4 / IPv6 Address)

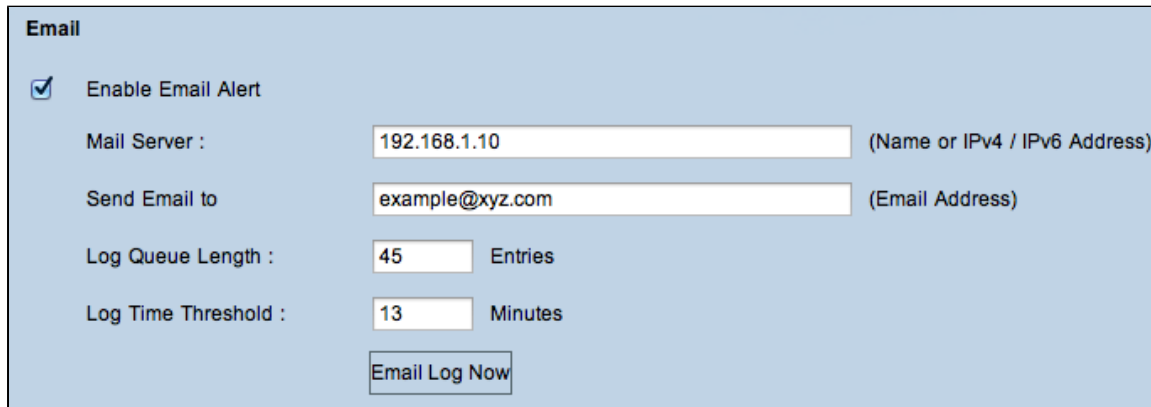
Schritt 2: Aktivieren Sie das Kontrollkästchen **Enable Syslog** (Syslog aktivieren), um den Syslog-Dienst auf dem Gerät zu aktivieren.

Timesaver: Fahren Sie mit Schritt 4 fort, wenn Syslog deaktiviert werden muss.

Schritt 3: Geben Sie den Domännennamen oder die IP-Adresse des Syslog-Servers in das Feld Syslog-Server ein.

E-Mail

In diesem Abschnitt wird erläutert, wie der Router bei der Protokollierung von Ereignissen E-Mail-Warnmeldungen senden kann.



Email

Enable Email Alert

Mail Server : (Name or IPv4 / IPv6 Address)

Send Email to (Email Address)

Log Queue Length : Entries

Log Time Threshold : Minutes

Schritt 4: Aktivieren Sie **E-Mail-Warnmeldung aktivieren**, um die Funktion zu aktivieren. Dadurch kann der Router E-Mail-Warnmeldungen an die vom Benutzer angegebene E-Mail-Adresse senden.

Zeitersparnis: Fahren Sie mit Schritt 10 fort, wenn die E-Mail-Warnmeldung deaktiviert werden muss.

Schritt 5: Geben Sie die IPv4- oder IPv6-Adresse des SMTP-Servers Ihres ISP in das Feld Mail-Server ein.

Hinweis: Möglicherweise müssen Sie Ihren Router mit einem Hostnamen identifizieren. Wählen Sie **Setup > Network** (Setup > Netzwerk), um den Hostnamen des Routers festzulegen.

Schritt 6: Geben Sie im Feld E-Mail senden an die E-Mail-Adresse ein, an die die Warnungen gesendet werden sollen.

Schritt 7. Geben Sie im Feld Länge der Protokollwarteschlange die Anzahl der Protokolleinträge ein, die in die E-Mail aufgenommen werden sollen. Der Standardwert ist 50.

Schritt 8: Geben Sie in das Feld "Log Time Threshold" (Protokollzeitschwellenwert) die Anzahl der Minuten ein, die vor dem Senden des Protokolls Daten gesammelt werden sollen. Der Schwellenwert für die Protokollzeit ist die maximale Wartezeit, bevor eine E-Mail-Protokollmeldung gesendet wird. Wenn der Grenzwert für die Protokollzeit abläuft, wird eine E-Mail gesendet, unabhängig davon, ob der Puffer für das E-Mail-Protokoll voll ist. Der Standardwert ist 10 Minuten.

Schritt 9. (Optional) Klicken Sie auf **Jetzt anmelden**, um sofort eine Nachricht an die angegebene E-Mail-Adresse zu senden und die Einstellungen zu testen.

Protokolleinstellung

In diesem Abschnitt wird die Anzahl der Ereignisse erläutert, die in den Protokollen gemeldet werden können:

Log Setting

Alert Log

Syn Flooding
 IP Spoofing
 Win Nuke
 Ping Of Death
 Unauthorized Login Attempt

General Log

System Error Messages
 Deny Policies
 Allow Policies
 Configuration Changes
 Authorized Login

Schritt 10. Der Bereich "Warnmeldungsprotokoll" enthält häufige Angriffstypen und nicht authentifizierte Anmeldeversuche. Aktivieren Sie die Kontrollkästchen der gewünschten Angriffe, um sie in das Ereignisprotokoll aufzunehmen, oder deaktivieren Sie sie, um sie aus dem Ereignisprotokoll auszulassen.

âf» SYN-Flooding - Der Angreifer sendet kontinuierlich viele SYNC-Pakete, was dazu führt, dass der Router mehrere Sitzungen öffnet, sodass der Datenverkehr sehr voll wird und der Router legitimen Datenverkehr verweigert.

âf» IP-Spoofing - Der Angreifer sendet Pakete von einer gefälschten Quell-IP-Adresse, damit der Angriff wie legitimer Datenverkehr aussieht.

âf» Win Nuke - Der Angreifer sendet eine Out-of-Band-Nachricht an einen Windows-Computer, um den Zielcomputer zum Absturz zu bringen.

âf» Ping of Death - Der Angreifer sendet ein großes IP-Paket, um den Zielcomputer zum Absturz zu bringen.

âf» Nicht autorisierter Anmeldeversuch: Jemand hat versucht, sich beim Router-Konfigurationsprogramm ohne ordnungsgemäße Authentifizierung anzumelden.

Schritt 11. Der Bereich "Allgemeines Protokoll" umfasst die Aktionen zum Durchsetzen konfigurierter Richtlinien sowie Routineereignisse wie autorisierte Anmeldungen und Konfigurationsänderungen. Aktivieren Sie das Kontrollkästchen eines beliebigen Ereignisses, um es in das allgemeine Protokoll aufzunehmen. Deaktivieren Sie das Kontrollkästchen, um es aus dem allgemeinen Protokoll zu entfernen.

âf» Systemfehlermeldungen - Alle Systemfehlermeldungen.

âf» Richtlinien verweigern - Instanzen, in denen der Router den Zugriff basierend auf Ihren Zugriffsregeln verweigert hat.

âf» Zulassen von Richtlinien - Instanzen, in denen der Router den Zugriff basierend auf Ihren Zugriffsregeln genehmigte.

âf» Konfigurationsänderungen - Instanzen, in denen Änderungen in der Konfiguration gespeichert wurden.

âf» Autorisierte Anmeldung - Instanzen, wenn sich jemand erfolgreich beim Router-Konfigurationsprogramm angemeldet hat, nachdem er den richtigen Benutzernamen und das richtige Kennwort eingegeben hat.

âf» Output Blocking Event (Ausgabe-Blockierungsereignis): Instanzen, bei denen ein Ereignis in der ProtectLink-Webreputation oder der URL-Filterung auftritt.

Hinweis: Das Ereignis zur Ausgangsblockierung ist nur auf RV082-VPN-Routern verfügbar.

Log Setting

Alert Log

Syn Flooding IP Spoofing Win Nuke

Ping Of Death Unauthorized Login Attempt

General Log

System Error Messages Deny Policies Allow Policies

Configuration Changes Authorized Login

View System Log **Outgoing Log Table** **Incoming Log Table** **Clear Log**

Save **Cancel**

Schritt 12: (Optional) Um das Systemprotokoll anzuzeigen, klicken Sie auf **Systemprotokoll anzeigen**. Das Fenster *Systemprotokoll* wird angezeigt:

Current Time : Fri Jan 1 02:53:56 2010

Time	Event-Type	Message
Jan 1 04:18:02 2010	System Log	HTTP Basic authentication success for user: admin
Jan 1 05:38:06 2010	System Log	HTTP Basic authentication success for user: admin
Jan 1 00:00:05 2010	System Log	router79f37a : System is up
Jan 1 00:04:42 2010	System Log	HTTP Basic authentication success for user: admin
Jan 1 02:53:40 2010	System Log	HTTP Basic authentication success for user: admin

Hinweis: Protokolleinträge enthalten das Datum und die Uhrzeit des Ereignistyps sowie eine Meldung. Diese Meldung gibt den Richtlinientyp an, z. B. Zugriffsregel, LAN-IP-Adresse der Quelle und MAC-Adresse.

Schritt 13: Wählen Sie ein bestimmtes Protokoll aus der Dropdown-Liste aus.

Schritt 14. (Optional) Klicken Sie auf **Aktualisieren**, um die Daten zu aktualisieren.

Schritt 15. (Optional) Um alle angezeigten Informationen zu löschen, klicken Sie auf **Löschen**.

Schritt 16: Klicken Sie auf **Schließen**, um das Fenster zu schließen.

Log Setting

Alert Log

Syn Flooding IP Spoofing Win Nuke

Ping Of Death Unauthorized Login Attempt

General Log

System Error Messages Deny Policies Allow Policies

Configuration Changes Authorized Login

View System Log **Outgoing Log Table** Incoming Log Table Clear Log

Save Cancel

Schritt 17: (Optional) Um die Informationen zu den ausgehenden Paketen anzuzeigen, klicken Sie auf **Tabelle für ausgehende Protokolle**. Die Informationen werden in einem neuen Fenster angezeigt.

Time	Event-Type	Message
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52416->74.125.227.113:443 on eth1
Jul 16 13:24:17 2013	Connection Accepted	TCP 192.168.1.100:52415->69.171.248.16:443 on eth1
Jul 16 13:24:19 2013	Connection Accepted	TCP 192.168.1.100:52436->157.55.240.222:443 on eth1
Jul 16 13:24:20 2013	Connection Accepted	TCP 192.168.1.100:52437->157.55.240.222:443 on eth1
Jul 16 13:24:29 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:29 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:30 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:31 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:31 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:33 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1
Jul 16 13:24:33 2013	Connection Accepted	TCP 192.168.1.100:52458->164.113.67.8:80 on eth1

Schritt 18. (Optional) Um die Daten zu aktualisieren, klicken Sie auf **Aktualisieren**.

Schritt 19: Klicken Sie auf **Schließen**, um das Fenster zu schließen.

Log Setting

Alert Log

Syn Flooding IP Spoofing Win Nuke

Ping Of Death Unauthorized Login Attempt

General Log

System Error Messages Deny Policies Allow Policies

Configuration Changes Authorized Login

View System Log Outgoing Log Table **Incoming Log Table** Clear Log

Save Cancel

Schritt 20. (Optional) Klicken Sie auf **Incoming Log Table**, um die Informationen über die eingehenden Pakete anzuzeigen. Die Informationen werden in einem neuen Fenster geöffnet. Wenn eine Warnung über das Popup-Fenster angezeigt wird, lassen Sie den gesperrten Inhalt zu.

Current Time : Tue Jul 16 20:55:23 2013 Refresh

Time	Event-Type	Message
Jul 16 20:55:13 2013	Connection Accepted	ICMP type 0 code 0 10.1.1.2->192.168.1.13 on eth0
Jul 16 20:55:14 2013	Connection Accepted	ICMP type 0 code 0 10.1.1.2->192.168.1.13 on eth0
Jul 16 20:55:15 2013	Connection Accepted	ICMP type 0 code 0 10.1.1.2->192.168.1.13 on eth0
Jul 16 20:55:16 2013	Connection Accepted	ICMP type 0 code 0 10.1.1.2->192.168.1.13 on eth0

Schritt 21. (Optional) Um die Daten zu aktualisieren, klicken Sie auf **Aktualisieren**.

Schritt 22: Klicken Sie auf **Schließen**, um das Fenster zu schließen.

Log Setting

Alert Log

Syn Flooding IP Spoofing Win Nuke

Ping Of Death Unauthorized Login Attempt

General Log

System Error Messages Deny Policies Allow Policies

Configuration Changes Authorized Login

View System Log Outgoing Log Table Incoming Log Table **Clear Log**

Save Cancel

Schritt 23. (Optional) Um das Protokoll zu löschen, klicken Sie auf **Protokoll jetzt löschen**. Klicken

Sie nur dann auf diese Schaltfläche, wenn die Informationen in Zukunft nicht mehr angezeigt werden müssen.

Schritt 24: Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.