Winco Talk Manager

Agente WTM para WhatsApp:

Informações sobre conectividade e configurações de segurança

Data: 02 de junho de 2021
Autor: Ariel Marcelo Nigri
Versão do Agente: 1.4.3

Introdução

Este documento tem por objetivo explicar as necessidades de conectividade do Agente Winco Talk Manager para WhatsApp ("Agente WTM - Whatsapp"), assim como propor soluções para vários cenários de rede, identificação do tráfego e, por fim, segurança, ao permitir o acesso aos sistemas do Winco Talk Manager ao mesmo tempo em que se bloqueia outros acessos ao WhatsApp via navegador.

URLs e protocolos utilizados

Apresentamos a seguir a lista de todas as URLs usadas pelo Agente WTM - Whatsapp na sua comunicação com a internet. Todos os acessos ocorrem na porta **443**, que é padrão para HTTPS.

O acesso se inicia com um login na URL ***https://talkmanager.net*** seguido da chamada da aplicação do WhatsApp para Web, que fica na URL ***https://web.whatsapp.com/***. Daí em diante todo o acesso é controlado pela aplicação do WhatsApp para Web, sem interferência do Agente WTM - Whatsapp.

1. ***.talkmanager.net**: todos os acessos feitos pelo Agente WTM - Whatsapp para gerenciamento e acesso do sistema Cloud são feitos para hosts localizados no domínio "talkmanager.net" e são feitos no protocolo HTTPS convencional.
2. ***.whatsapp.com**: nesta URL fica a aplicação padrão do WhatsApp para Web, que é a base do programa Agente WTM - Whatsapp. Todos os acessos feitos para esta URL seguem estritamente o protocolo HTTPS, mas algumas utilizam o sub-protocolo **WebSockets** (wss://).
3. ***.whatsapp.net**: estas URLs de serviço do WhatsApp são utilizadas em várias situações, como para upload e download de arquivos de mídia criptografados. Apesar de todos os acessos ocorrerem na porta 443, alguns dos acessos não utilizam o protocolo HTTPS. Isso pode vir a causar problemas em alguns firewalls mais limitados, mas não há nada que possa ser feito pela Winco já que é uma característica do próprio WhatsApp.
4. ***.fbcdn.net**: estas URLs são utilizadas para visualização de fotos e mídias em geral e pertencem à rede de distribuição de conteúdo do Facebook, que é o proprietário do WhatsApp ("fbcdn" significa *Facebook Content Distribution Network*).

Nota: As regras do firewall devem ser criadas por URL/HOST e não por IP, pois as listas de IPs podem mudar sem aviso prévio.

Configurações de proxy e de autenticação

Por padrão, o Agente WTM - Whatsapp utiliza as configurações padrão de proxy HTTPS do computador para acessar a internet. Estas configurações ficam nas “definições de rede e internet” no caso de sistemas operacionais Windows.

Assim como as configurações de proxy, a autenticação também é respeitada pelo Agente WTM - Whatsapp. Caso a rede utilize autenticação transparente do tipo NTLM ou NEGOTIATE, o Agente WTM - Whatsapp se autenticará automaticamente.

Sobrescrevendo as Configurações de Proxy

Quando necessário, as configurações de proxy do computador podem ser sobrescritas para uso específico do Agente WTM - Whatsapp. Por uma questão de segurança, porém, não é permitido ao usuário final mexer na configuração do proxy, que é feita diretamente na *registry* (e por isso pode ser distribuída via *policy* no AD).

As configurações de proxy do Agente WTM - Whatsapp ficam nas seguintes chaves (respectivamente para Windows 64bits e para Windows 32bits):

- `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Winco\WtmWpp\`
- `HKEY_LOCAL_MACHINE\Software\Winco\WtmWpp`

Obs.: Crie estas chaves caso ainda não existam.

Para definir um proxy específico para o Agente WTM - Whatsapp, crie uma nova entrada do tipo VALOR:

Tipo: `String`
Nome: `proxy_server`
Dado: `<proxy_ip>:<proxy_port>` ← Exemplo: **192.168.0.1:8080**

Para desativar o acesso via proxy num computador que tenha o proxy como padrão configurado nas definições de internet, preencha como "Dado" a palavra ***none*** em minúsculas.

Nota: Recomendamos definir o mesmo VALOR igualmente nas duas chaves (de 32 e 64 bits) em todos os computadores 64 bits, pois no futuro poderemos voltar a distribuir versões 64 bits da aplicação.

Instalando as configurações de Proxy

A distribuição de valores e chaves da *registry* pode ser feita manualmente, via arquivo ou via Microsoft Active Directory. Qualquer que seja o método, é necessário ser administrador do computador ou da rede para poder escrever na chave de registry **HKEY_LOCAL_MACHINE**.

As 3 formas de alterar a *registry* são:

1. Manualmente: utilizando as ferramentas REGEDIT (gráfica) ou REG.EXE (linha de comando).

2. Via arquivo: Após configurar um computador corretamente, exporte a chave configurada utilizando a opção de exportar chave de registro para um arquivo *.REG*. Uma vez criado o arquivo, para instalar as mesmas configurações em outro computador basta copiá-lo e executá-lo no computador de destino.

3. Via criação de Group Policy Objects: Para redes controladas por MS Active Directory, pode-se distribuir as chaves de registry do Agente WTM - Whatsapp como qualquer outra chave.

Identificação do Agente WTM - Whatsapp

Além da mudança na configuração de proxy, há outras formas de diferenciar o tráfego originado do Agente WTM Wpp, de modo a permitir a sua utilização na rede, como descrito a seguir:

Pelo executável da aplicação

Todo o acesso à internet para o funcionamento do Agente WTM - Whatsapp é feito a partir do executável principal.

Na versão Windows, o programa se chama ***WtmWpp.exe***, cuja descrição é *"WTM for WhatsApp"*, e que é assinado digitalmente pela Winco Sistemas.

Nas versões Linux e Mac OS, o nome do executável é ***wtmwpp***, e a assinatura vai só no pacote e não no executável (como é normal nestas plataformas).

Pelos cabeçalhos (headers) HTTP

Existem 2 locais onde se pode identificar o Agente WTM - Whatsapp inspecionando-se os cabeçalhos HTTP:

1. Pelo cabeçalho ***User-agent***: A string de User-Agent, que é um cabeçalho padrão HTTP, inclui a versão do programa. Note que este cabeçalho é enviado nas requisições via PROXY HTTPS ainda na parte '*não criptografada*' do protocolo, o que permite sua identificação mesmo em servidores PROXY sem inspeção de SSL ou HTTPS.

2. Pelo cabeçalho proprietário ***X-Winco-WTMWPP***: Todos as requisições HTTPS do cliente WTM para WhatsApp utilizam um cabeçalho proprietário que contém a versão da aplicação.

Ambas as identificações podem ser visualizadas abaixo, neste exemplo de um cabeçalho real enviado pelo Agente WTM - Whatsapp. Os textos de identificação do WTM estão marcados em **AZUL**:

```
GET / HTTP/1.1
Host: web.whatsapp.com
accept: text/html,application/xhtml+xml,application/xml;q=0.9,
image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
accept-encoding: gzip, deflate, br
accept-language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7,es;q=0.6
cache-control: no-cache
cookie: wa_lang_pref=pt_br
pragma: no-cache
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) WtmWpp/1.4.2
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
X-Winco-WTMWPP: 1.4.2
```

Cenários de configuração

Enumeramos abaixo os cenários mais comuns de configuração de rede e as formas de implantação mais adequadas, a nosso ver, para cada rede.

Esta lista não se propõe a esgotar o assunto e também não representa uma diretiva, mas apenas uma sugestão. Baseando-se nas informações fornecidas na seção anterior, os administradores de rede podem planejar outras topologias.

Redes sem restrição de acesso ao WhatsApp

Se o acesso ao WhatsApp for permitido na rede onde serão instalados os Agente WTM - Whatsapp, então normalmente não haverá problemas e tudo deverá funcionar como esperado.

Por uma questão de depuração, caso ocorra algum problema com o Agente WTM - Whatsapp, deve-se seguir as recomendações do próprio WhatsApp quanto a configuração. Este teste deve ser feito utilizando-se o WhatsApp Web (https://web.whatsapp.com).

Além deste acesso só será necessário testar o acesso ao domínio do Winco Talk Manager (https://talkmanager.net) e tudo estará pronto para a produção.

Redes com inspeção HTTPS ou regras de acesso por executável

Como explicado acima, o Agente WTM - Whatsapp é facilmente identificável. Tanto o executável que acessa, quanto a sua requisição HTTPS.

Portanto, para redes com capacidade de verificação de executáveis ou certificados, basta incluir na *whitelist* (ou *permission list*, se preferir) o certificado da Winco Sistemas, o nome do executável, sua localização, ou sua descrição.
Da mesma forma, em redes que têm controle HTTPS, pode-se identificar todas as requisições HTTPS do

Agente WTM - Whatsapp de forma simples e, assim, usar essa informação para permitir o acesso à internet.

Redes sem inspeção HTTPS e com proxy obrigatório

Há 3 opções neste caso:

1) Configurando o User Agent

Alguns proxies/sistemas de controle de acesso permitem configurar o bloqueio de acesso à internet definindo-se uma lista proibida e/ou permitida de "User Agents", que são os navegadores e outras aplicações que têm direitos a acessar a internet.

Para fazer a configuração utilize as definições apresentadas no tópico anterior "Identificação do Agente WTM - Whatsapp ", "Pelos cabeçalhos HTTP", e consulte a documentação do fabricante do filtro de conteúdo/proxy/firewall.

2) Criando uma saída direta pelo firewall, onde somente o Agente WTM - Whatsapp **fica dispensado de usar proxy**

A opção para redes onde não há como limitar o "User Agent", é tirar a definição de PROXY apenas do Agente WTM - Whatsapp enquanto que todos os outros processos ainda serão obrigados a acessar via proxy. Em seguida libera-se no firewall o acesso direto às URLs de serviço listadas no início do documento.

A desvantagem deste método é que o usuário poderá tentar instalar no computador programas com direitos de usuário que acessem diretamente a rede WhatsApp e que, portanto, poderão driblar a segurança da rede. Mesmo sendo uma possibilidade remota, é uma possibilidade.

3) Criando um proxy específico para o acesso WhatsApp e configurando este proxy como documentado acima

Esta opção é a mesma que existe para redes sem proxy e será explicada a seguir.

Redes sem inspeção HTTPS e sem proxy obrigatório

Neste cenário, a única opção que existe para proibir o acesso ao WhatsApp utilizando-se a interface web enquanto se permite o acesso via Agente WTM - Whatsapp é bloquear os acessos ao WhatsApp no firewall da rede e direcionar os acessos feitos pelo Agente WTM - Whatsapp para um proxy específico.

Este proxy pode ficar na mesma rede do cliente ou na nuvem, sendo que deve ser implementada uma autenticação entre o proxy e o Agente WTM - Whatsapp para evitar acessos espúrios. Se for utilizado um proxy local a autenticação poderá ser feita de forma simples e transparente utilizando-se o protocolo NTLM ou NEGOTIATE.

Por último, deve-se configurar este proxy para só acessar as URLs de serviço do Agente WTM, de forma a restringir ainda mais o uso não autorizado.